面 向 2 1 世 纪 课 程 教 材

Textbook Series for 21st

代数学引论

第二版

聂灵沼　丁石孙　著



高等教育出版社
HIGHER EDUCATION PRESS

内容提要

本书是教育部"高等教育面向21世纪教学内容和课程体系改革计划"的研究成果，是面向21世纪课程教材。本书是作者根据多年教学经验，在原有讲义基础上经过修改、补充而成的。书中介绍了代数学的基本知识：第一至第七章给出群、环、模、域四个基本的代数结构及其性质；第八章介绍伽罗瓦理论；第九章是多重线性代数初步。各章后配有相当数量的习题。全书相当于一学年课程的教材。

本书取材恰当，论证严谨，文字简洁、流畅。

第二版除进行少量文字修改外，对习题作了一些调整，较难的习题用星号标出，并给以适当的提示。

本书可用作高等学校数学系抽象代数课的教材，也可供其他相关专业的师生参考。

图书在版编目(CIP)数据

代数学引论/聂灵沼、丁石孙著.—2版.—北京：高等教育出版社，2000（2002重印）

ISBN 7-04-008893-2

Ⅰ.代… Ⅱ.聂… Ⅲ.代数-概论 Ⅳ.015

中国版本图书馆CIP数据核字(2000)第67140号

代数学引论 第二版

聂灵沼 丁石孙 著

出版发行 高等教育出版社

社 址 北京市东城区沙滩后街55号 邮政编码 100009

电 话 010-64054588 传 真 010-64014048

网 址 http://www.hep.edu.cn

经 销 新华书店北京发行所

排 版 高等教育出版社照排中心

印 刷 国防工业出版社印刷厂

开 本 787×960 1/16 版 次 1988年3月第1版

2000年9月第2版

印 张 22 印 次 2002年4月第2次印刷

字 数 385 000 定 价 18.70元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

第二版序言

本书的第一版是我们在几年的教学基础上编写的，其中的若干不当之处在第二次印刷中作了更正. 尽管如此，书中仍存在一些问题，如某些词句和个别习题叙述欠妥，少量难度较大的习题不适于多数使用者等. 针对这些问题，我们作了必要的文字上的修改，较难的习题用星号标出，以及给以适当的提示. 赵春来教授曾两次使用过此教材，也发现一些不当之处. 第二版是经赵春来教授修改而成的. 作者衷心感谢所有的使用者对于本版提出进一步的意见.

作者

2000 年 3 月

前言

本书是从我们近几年编写的讲义经过修改、补充而成的，目的是介绍代数学最基本的知识.

群、环、模与域是四个基本的代数结构. 对于它们的了解不但一般数学工作者是必要的，对于要用代数的科学工作者也是必要的. 我们在第一章到第七章中给出了这四个代数结构的基本性质. 第八章简单地介绍了伽罗瓦理论，我们认为这是一般数学工作者应该掌握的知识. 第九章对多重线性代数作了初步的介绍. 多重线性代数应该是线性代数的一部分，不过根据我们的经验，要真正理解这部分内容需要一定的数学的成熟性，因之，放在本书的最后供读者参考. 初等数论和集合论的某些知识是学习代数的必要的准备，考虑到不同的读者对它们有不同程度的了解，因之在第零章中我们罗列了这两方面必要的事实.

本书的取材大体上相当于一个学年课程的教材. 当然，如果用作教材，那么教师可以根据学生的情况适当选取其中的一部分. 譬如，在学生已经掌握了第一章的内容之后，第二章到第七章的内容可以安排成一个学期课程；或者，在学生掌握了必要的群、环、模的知识之后，第七、八章可以用作介绍伽罗瓦理论的教材.

每一章都附有足够数量的习题，其中大部分是基本的，也有少量的难度较大. 读者可以选择一部分来做.

本书的初稿在北京大学数学系已用过多次，每次用完后都作了修改，我们始终是不很满意的. 今天整理出来正式出版，并不是由于我们认为它已经是一本成熟的教材，而是考虑到目前这样一个内容的参考书太少，拿出来对于学习代数的人可能有些好处. 我们希望在有更多的人使用的基础上作进一步的修改.

本书的初稿及逐年的修改稿在北京大学数学系讲授过程中，石生明、蓝以中、丘维声等同志提出过宝贵的修改意见. 在最后定稿前，南京大学周伯壎先生仔细审阅了全书，提出了很好的意见. 对他们的帮助，我们表示衷心的感谢.

作者于北京大学中关园
1987 年 2 月

责任编辑　胡乃冏
封面设计　张　楠
责任绘图　何　青
版式设计　何　青
责任校对　项如英
责任印制　杨　明

目 录

第零章　集合与整数

集合是数学的基本概念之一. 它是具有一定属性的事物形成的一个集体. 根据这属性可以区别一个事物属于或不属于这个集合. 例如空间的点集、实系数多项式集合、定义在区间 $[0,1]$ 上的实函数集合等. 本章主要讨论一个集合上的等价关系、偏序关系以及整数的算术性质. 关于集合的子集、交集、并集以及一个集合到另一个集合的映射等概念, 在高等代数课程中已有介绍, 这里不再重复.

§1　集合上的等价关系

在一个集合的元素之间常常存在某种关系. 例如, 两个 $n\times n$ 的复矩阵的相似或不相似; 空间两直线平行或不平行; 数学分析中两个柯西序列的等价或不等价, 都是特殊集合上的重要关系.

设 S 为一非空集合, $a,b,c,\cdots$ 表示它的元素. 设在 S 中任意两个元素之间存在 (或不存在) 某种属性 R. 只要 R 满足下面的条件, 即对于 S 中任一对有次序的元素 a,b 来说, a,b 有这种属性 R 或者 a,b 没有这种属性 R, 这两者必定有一成立而且只有一成立, 那么我们说 R 是集合 S 上的一个**二元关系**, 或简称**关系**. 若 a,b 有关系 R, 则记作 aRb.

上面列举的"相似"、"平行"和"等价"都是它们的相应集合上的二元关系. 又如, 实数集合上的大小关系"$\leq$", 整数集合上的整除关系 $a|b$ 都是该集合上的二元关系. 再如一个非空集合 S 中元素之间的相等 (或不相等), 子集之间的包含 (或不包含) 分别是 S 上和 S 的幂集 $P(S)$ 上的二元关系. 所谓 S 的**幂集** $P(S)$ 就是 S 的所有子集作元素构成的集合.

非空集合 S 上一个二元关系 R 还可用笛卡尔积 $S\times S$ 的一个子集 T 表示. T 规定如下

$$T=\{(a,b)\in S\times S\,|\,a,b\text{有关系}R\}.$$

于是可以说, 元素 a,b 有关系 R 当且仅当 $(a,b)\in T$. T 称为关系 R 在 $S\times S$ 中的**图象**. 反之, $S\times S$ 的任一子集 T 可以给出 S 上的一个二元关系 R: 称元素 a,b 有关系 R 当且仅当 $(a,b)\in T$. 由此可知 R 满足二元关系的条件.

按照矩阵的相似关系可以将 $n\times n$ 复矩阵分成若干相似类, 使之每一类有一个标准形作为代表; 按照柯西序列的等价关系可以将柯西序列分成一些等价类, 使之每一类代表一个实数. 这些都是数学中常见的基本方法. "相似"和"等价", 它们有三条共性, 就是反身性、对称性和传递性.

定义 1 如果一个非空集合 S 的一个二元关系 R 满足下列三条:

1) 反身性 $a R a$, 对所有 $a \in S$;

2) 对称性 若 $a R b$, 则 $b R a$;

3) 传递性 若 $a R b$ 且 $b R c$, 则 $a R c$;

则称 R 是 S 的一个 **等价关系**. 等价关系 R 通常记成 "$\sim$".

显然, "相似"、"平行"、"柯西序列等价" 都是等价关系. 但是 "$\leq$" 和 "$a|b$" 则不是等价关系. 而 "$=$" 和 "$a|b$ 且 $b|a$" 是等价关系.

如果非空集合 S 的一组子集 $\{S_\lambda \mid \lambda \in I\}$, I 为指标集, 满足下列条件:

1) $S = \bigcup\limits_{\lambda \in I} S_\lambda$;

2) $S_\lambda \cap S_\mu = \emptyset, \lambda \neq \mu, \lambda, \mu \in I$;

则 $\{S_\lambda\}$ 叫做 S 的一个 **划分**.

非空集合 S 的任一个等价关系 $\sim$ 确定 S 的一个划分如下: 对每个元素 $a \in S$, 规定

$$S_a = \{x \in S \mid x \sim a\},$$

这样得到 S 的一组子集 $\{S_a \mid a \in S\}$. 证明它是 S 的一个划分. 首先, 由于反身性, $a \sim a$, 所以 $a \in S_a$, 于是 $S = \bigcup\limits_{a \in S} S_a$. 其次证明, 若 $S_a \cap S_b \neq \emptyset$, 则 $a \sim b$ 且 $S_a = S_b$. 设 $S_a \cap S_b \neq \emptyset$, 取一个 $c \in S_a \cap S_b$, 于是 $c \sim a, c \sim b$, 由对称性, $a \sim c$, 再由传递性, 得 $a \sim b$. 其次对任一元素 $x \in S_a$, 有 $x \sim a$, 由传递性得 $x \sim b$, 从而 $x \in S_b$, 所以 $S_a \subset S_b$. 再由对称性, $b \sim a$, 同理得 $S_b \subset S_a$. 所以 $S_a = S_b$. 由此可知 $\{S_a \mid a \in S\}$, 把重复的去掉之后, 就是 S 的一个划分. 这个划分中的每个元素叫做由等价关系确定的 **等价类**.

反之, S 的任一个划分 $\{S_\lambda \mid \lambda \in I\}$ 决定一个等价关系如下: 规定

$$a \sim b \iff a, b \text{属于同一个} S_\lambda.$$

首先, 由划分的定义可知 a, b 属于同一个 S_λ 或者 a, b 分属于不同的 S_λ, 这两者有一而且只有一成立. 因而 "$\sim$" 是一个二元关系. 进一步由划分的定义, 读者不难证明, "$\sim$" 是一个等价关系, 而且这个等价关系如上决定的划分就是原来的划分.

一个集合的等价关系的重要性在于由它可以产生出新的集合. 设 "$\sim$" 是非空集合 S 的一个等价关系. 如上, "$\sim$" 将 S 分成一些互不相交的等价类 $\{S_\lambda \mid \lambda \in I\}$ 的并. 为表法简明起见, 在每个等价类 S_λ 中取一个代表 a, 将 S_λ 写成 $\overline{a}$. 这种表示与代表的取法无关, 就是说, $\overline{a} = \overline{b}$ 当且仅当 $a \sim b$. 用这些等价类 $\overline{a}, \overline{b}, \cdots$ 作元素得到一个新的集合, 记作 $S/\sim$, 叫做 S 关于等价关系 $\sim$ 的

商集. 今后将会看到，对于各种不同的具体集合 S 和等价关系 $\sim$, 商集 $S/\sim$ 将会有它崭新的意义.

例 三维仿射空间的直线集合按平行关系分成一些平行直线束，设想每一平行直线束相交于同一个无穷远点. 这样，以平行直线束为元素得到的商集就表示一个无穷远平面，它是一个射影平面. 把这个射影平面添加到三维仿射空间就得到一个三维射影空间. 这就是历史上将仿射空间扩充成射影空间的朴素的几何直观的方法.

集合 S 到商集 $S/\sim$ 存在一个 **自然映射**

$$\nu : x \mapsto \overline{x},\ x \in S.$$

它是一个满射，而且 $\nu(a) = \nu(b)$ 当且仅当 $a \sim b$.

反之，设 φ 是集合 S 到集合 T 的一个映射. 于是在 S 上可以如下定义一个关系 $\sim$:

$$a \sim b \text{ 当且仅当 } \varphi(a) = \varphi(b),\ a, b \in S.$$

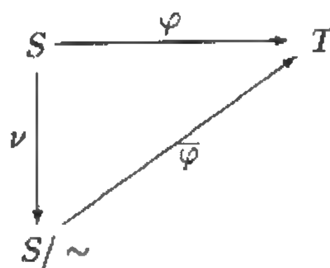
容易看出，这是一个等价关系. 而且 φ 诱导出商集 $S/\sim$ 到 T 的一个映射 $\overline{\varphi}$ 如下:

$$\overline{\varphi}(\overline{x}) = \varphi(x),\ x \in S.$$

显然 $\overline{\varphi}$ 是单一的. 这样，映射 φ 就分解成一个自然映射 $\nu : S \to S/\sim$ 和一个单射 $\overline{\varphi}$ 的积

$$\varphi = \overline{\varphi} \cdot \nu.$$

用图表示就是



综上所述，我们得到

定理 1 非空集合 S 上的一个等价关系 $\sim$ 决定 S 对 $\sim$ 的一个商集 $S/\sim$, 并诱导出一个自然映射 $\nu : S \to S/\sim$ 使得 $x \sim y,\ x, y \in S \iff \nu(x) = \nu(y)$. 反之，任一个集合映射 $\varphi : S \to T$ 决定 S 上的一个等价关系 $\sim$ 使得 $x \sim y,\ x, y \in S \iff \varphi(x) = \varphi(y)$. 而且 φ 诱导出商集 $S/\sim$ 到 T 的单一映射 $\overline{\varphi} : \overline{\varphi}(\overline{x}) = \varphi(x),\ x \in S$, 使得 φ 有分解

$$\varphi = \overline{\varphi} \cdot \nu.$$

§2 自然数

自然数系是由 $0, 1, 2, \cdots$ 组成的，记作 $\mathbf{N}$. 自然数在代数中是基本的，人们首先认识的是自然数，然后才逐渐认识整数、有理数、实数和复数. 自然数系是可数无限集合的一个原型. 它的良序性质是数学归纳法原理的依据. 自然数系的整除性和素数的研究促使了数论的发展. 用**佩阿诺 (Peano) 公理**来描述自然数，容易使我们看清自然数的本质.

自然数系是这样一个非空集合 $\mathbf{N}$, 其中有一个选定了的元素 0, 和一个 $\mathbf{N}$ 到自身的后继映射 $a \mapsto a^+$, a^+ 叫做 a 的后继，满足

1) 映射 $a \mapsto a^+$ 是单一的，即从 $a^+ = b^+$ 推出 $a = b$;

2) 0 不是任何元素的后继，即不存在 $a \in \mathbf{N}$ 使得 $a^+ = 0$;

3) 如果 $\mathbf{N}$ 的任一个子集 S 满足 i) $0 \in S$ 而且 ii) 对所有元素 $a \in \mathbf{N}$, 从 $a \in S$ 恒有 $a^+ \in S$, 则 $S = \mathbf{N}$.

从公理 1) 和 2) 推出 $\mathbf{N}$ 是一个无穷集合，公理 3) 就是**数学归纳法原理**. 它是归纳法证明方法的基础. 设 $P(n)$ 是关于自然数 n 的某种性质或陈述，为了证明 $P(n)$ 对所有自然数是真的，我们只需证明两点： (1) $P(0)$ 是真的； (2) 若对任一自然数 n, $P(n)$ 是真的，则 $P(n^+)$ 也是真的. 于是根据数学归纳法原理， $P(n)$ 对所有自然数都是真的.

关于自然数的许多性质都可以应用数学归纳法原理予以证明. 例如，我们可以应用数学归纳法原理证明命题： $\mathbf{N}$ 的每个非零自然数 a 都是另一个自然数 b 的后继. 设 $S_1 = \{x \in \mathbf{N} \mid 对 x 存在一个 y \in \mathbf{N} 使得 x = y^+\}$, $S = \{0\} \cup S_1$. 证明 $S = \mathbf{N}$. 首先 $0 \in S$, 而且若 $b \in S$, 根据 S 的定义 $b^+ \in S$. 根据数学归纳法原理 $S = \mathbf{N}$.

归纳法的证明为大家所熟悉，但是归纳法或归纳法构造，则不大为大家所熟悉. 归纳法构造是以下列定理为基础的.

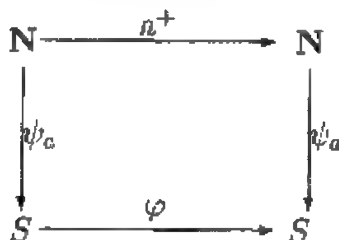
递归定理 *设 S 为一集合，φ 为 S 到自身的一个映射，a 为 S 的一个给定的元素. 则存在一个唯一的 $\mathbf{N}$ 到 S 的映射 ψ_a 使得*

$$\psi_a(0) = a$$

且

$$\psi_a(n^+) = \varphi(\psi_a(n)),\ n \in \mathbf{N}.$$

就是说下图交换



且

$$\psi_a(0) = a.$$

(交换图的概念可见第一章 §7.)

我们不打算给出这个定理的详细证明. 但是要说一下证明的思路. 一个集合 X 到另一个集合 Y 的任一个映射 f 规定了笛卡尔积 $X \times Y$ 的一个子集

$$T_f = \{(x, f(x)) \mid x \in X\}.$$

反之, $X \times Y$ 的一个子集 T 如果满足 1) 对每个 $x \in X$ 存在一个 $y \in Y$ 使 $(x,y) \in T$, 而且 2) 若 $(x,y),(x,y') \in T$, 则 $y = y'$, 那么 T 规定了一个映射 $f: X \to Y$ 使得 T 由所有的 $(x, f(x)), x \in X$ 组成. 基于这种看法, 我们考虑笛卡尔积 $\mathbf{N} \times S$ 的满足下列条件的子集 T: (1) $(0,a) \in T$, 而且 (2) 若 $(n,b) \in T$, 则 $(n^+, \varphi(b)) \in T$(对所有 $n \in \mathbf{N}$). 用 I 表示 $\mathbf{N} \times S$ 的所有这种子集的交. 读者可以根据自然数的公理证明 I 规定了一个映射 $\psi_a : \mathbf{N} \to S$, 而且 ψ_a 满足定理的要求. 不难证明, 满足定理要求的映射 ψ_a 是唯一的.

根据递归定理, 在自然数系上我们可以归纳地定义一个概念或归纳地构造一个函数. 自然数的加法和乘法的定义就是典型的例子.

定义 $\mathbf{N}$ 的加法如下: 对任意 $m, n \in \mathbf{N}$, 规定

$$m + 0 = m,$$

$$m + n^+ = (m + n)^+.$$

注意, 我们在递归定理中令 $S = \mathbf{N}$、$\varphi(n) = n^+, a = m$, 从而得到的映射 ψ_m 等于规定了加法运算, $\psi_m(n) = m + n$.

不难证明加法满足结合律、交换律和加法消去律. 将 0 的后继记成 $1, 0^+ = 1$, 于是有 $m + 1 = m^+$. 0 是加法的单位元素.

定义 $\mathbf{N}$ 的乘法如下: 对任意 $m, n \in \mathbf{N}$, 规定

$$m \cdot 0 = 0,$$

$$m \cdot n^+ = m \cdot n + m.$$

注意，在递归定理中我们令 $S=\mathbf{N},\varphi(n)=n+m,a=m$，从而得到的映射 ψ_m 等于规定了乘法运算，$\psi_m(n)=m\cdot n$.

不难证明乘法满足结合律、交换律、乘法消去律以及乘法对加法的分配律. 由定义可知 $m\cdot 1=m$，对所有自然数 m. 1 是乘法的单位元素.

自然数系还有一个**序**"$\leq$". 这个序规定了任意两个自然数 a,b 的大小. 我们说 $a\leq b$ 当且仅当 $a+x=b$ 在 $\mathbf{N}$ 内有解. 若 $a\leq b$ 且 $a\neq b$，则写成 $a<b$. $a\leq b$ 也可写成 $b\geq a$. 根据定义可知 $0\leq n, n<n^+$，对所有自然数 n. 关于序的一些性质在这里不一一列举了. 例如应用数学归纳法可以证明，对任一对自然数 n,n^+，不再存在自然数 m 满足 $n<m<n^+$. 因而从 $n<m$ 就可以断定 $n^+\leq m$. 特别值得提出的是

良序性质 *自然数系的任一非空子集 S 有一个最小元素，即存在一个 $m\in S$ 使得对所有 $x\in S$ 都有 $x\geq m$.*

证明 如果 S 包含 0，则 0 是 S 的最小元素. 假设：如果 S 包含 n，则 S 有一个最小元素. 由此证明，如果 S 包含 n^+，则 S 有一个最小元素. 作 $S'=S\cup\{n\}$. 根据归纳法假设，S' 有一个最小元素 m. 若 $m\in S$，则 m 就是 S 的最小元素. 假设 $m\notin S$，则必有 $m=n$，因而 $n\notin S$ 且 $n<a$，对所有的 $a\in S$. 于是，根据上面的说明可以断定 $n^-\leq a$ 对所有的 $a\in S$. 根据假设 $n^+\in S$，所以 n^+ 是 S 的最小元素. □

自然数系的良序性质是第二数学归纳法的基础.

第二数学归纳法 *假设 $P(n)$ 是关于自然数 n 的一种性质或陈述. 如果我们能够证明命题"若 $P(x)$ 对所有小于 n 的自然数 x 都真，则 $P(n)$ 也是真的"，其中包含 $P(0)$ 为真的证明. 那么可以断言 P 对所有自然数都是真的.*

证明 我们是在引号中的命题已被证明成立的前提下，来证明 P 对所有自然数 n 都真. 设 $S=\{x\in\mathbf{N}\mid P(x)\text{假}\}$. 求证 S 为空集. 反证法. 假如 S 非空，则 S 有一个最小自然数 m. 于是 $P(m)$ 假. 但是 $P(x)$ 对所有小于 m 的自然数都真. 这与上述命题矛盾. 所以 $S=\emptyset$. □

§3 整数、整数的整除性

我们知道在自然数系内方程 $a+x=b$ 有解当且仅当 $a\leq b$. 当 $a\leq b$ 时，这方程的解 x 记作 $b-a$，叫做 b 减 a 的差. 这意味着在自然数系内当 $b\geq a$ 时 b 减 a 有意义，$b-a$ 表示一个自然数，它是这方程的解，否则 $b-a$ 不能表示自然数，因而无意义. 为了使得自然数的差 $b-a$ 恒有意义，需要将自然数系加以扩充. 我们从经验得到启示，一个扩充的办法是引进"正"和"负"的概念. 当自然数 $b>a$ 时，$b-a$ 表示正整数，若 $b<a$ 时，$b-a$ 表示负整数. 为了

从数学上统一处理，我们的作法如下：

作自然数系的笛卡尔积 $\mathbf{N}\times\mathbf{N}=\{(a,b)\,|\,a,b\in\mathbf{N}\}$. (a,b) 意味着自然数 a,b 的差 $a-b$. 由于有不同的 (a,b) 表示同一个差，就需要在 $\mathbf{N}\times\mathbf{N}$ 中引进一个等价关系 $\sim$:

$$(a,b)\sim(c,d)\iff a+d=b+c.$$

容易验证这是一个等价关系. 包含 (a,b) 的等价类记作 $\overline{(a,b)}$. 商集 $\mathbf{N}\times\mathbf{N}/\sim$ 记作 $\mathbf{Z}$. 这就是我们的 **整数** 集合. 在 $\mathbf{Z}$ 内定义加法和乘法如下：

$$\overline{(a,b)}\oplus\overline{(c,d)}=\overline{(a+c,b+d)},$$

$$\overline{(a,b)}\odot\overline{(c,d)}=\overline{(ac+bd,ad+bc)}.$$

不难验证，上述定义与类的代表的取法无关. 由于自然数的运算满足交换律、结合律和分配律，那么整数集 $\mathbf{Z}$ 的运算也满足同样的运算规律，这是容易验证的. 此时 $\mathbf{Z}$ 称为整数环. 显然 $\overline{(0,0)}$ 是 $\mathbf{Z}$ 的零元素，$\overline{(1,0)}$ 是单位元素. 用 $\overline{(a,b)}$ 表示整数，符号未免累赘，需要简化. 当 $a\geq b$ 时，方程 $a=b+x$ 在自然数 $\mathbf{N}$ 中有唯一解 $x=n$. 于是 $\overline{(a,b)}$ 可以写成 $\overline{(n,0)}$. 当 $a<b$ 时，方程 $a+x=b$ 在 $\mathbf{N}$ 中有唯一解 $x=n$, 于是 $\overline{(a,b)}$ 可写成 $\overline{(0,n)}$. 当 $n>0$ 时，$\overline{(n,0)}$ 和 $\overline{(0,n)}$ 分别叫做 **正**、**负** 整数. 自然数系 $\mathbf{N}$ 到整数环 $\mathbf{Z}$ 有一个自然映射 $n\mapsto\overline{(n,0)}$, 它是单射而且保持加法和乘法，就是说，若 $n\mapsto\overline{(n,0)}, m\mapsto\overline{(m,0)}$, 则因 $\overline{(n+m,0)}=\overline{(n,0)}\odot\overline{(m,0)}$, $\overline{(n\cdot m,0)}=\overline{(n,0)}\odot\overline{(m,0)}$ 而有 $n+m\mapsto\overline{(n,0)}\oplus\overline{(m,0)}, n\cdot m\mapsto\overline{(n,0)}\odot\overline{(m,0)}$. 因此我们可以将自然数 n 与正整数 $\overline{(n,0)}$ 和零 $\overline{(0,0)}$ 等同，使得自然数系 $\mathbf{N}$ 成为整数环 $\mathbf{Z}$ 的一部分，而且 $\mathbf{N}$ 的加法和乘法在 $\mathbf{Z}$ 内仍然保持不变. 因此整数运算符号 $\oplus$ 和 $\odot$ 也可以简记成 + 和 $\cdot$, 负整数 $\overline{(0,n)}$ 可简单记成 $-n$. 于是非负整数的运算和自然数的运算相同. 负整数与负整数之间，负整数与非负整数之间的运算表示如下：

$$(-n)+(-m)=-(n+m),$$

$$n+(-m)=(-m)+n=\begin{cases} n-m, & \text{若}n\geq m,\\ -(m-n), & \text{若}n<m,\end{cases}$$

$$(-n)\cdot(-m)=n\cdot m,$$

$$n\cdot(-m)=(-m)\cdot n=-n\cdot m.$$

以后用 $a,b,c,\cdots$ 表示任意整数. 现在 $\mathbf{Z}$ 内引进负元素的概念. 对每个整数 a, 存在一个唯一的整数 b 使得 $a+b=0$. 因为，若 $a=n\in\mathbf{N}$, 则 $b=-n$; 若

$a=-n, n\in \mathbf{N}$, 则 $b=n$. b 叫做整数 a 的 **负元素**, 记成 $b=-a$, 同时 a 也是整数 $-a$ 的负元素, 因而有

$$-(-a)=a.$$

由上可知 $-a$ 是 a 的负元素, 但 $-a$ 不必是负整数. 负元素和负整数是两个不同的概念. 进而在 $\mathbf{Z}$ 内引进减法. 对任意两个整数 a,b, 规定

$$a-b=a+(-b).$$

最后, 一般方程 $a+x=b$ 在 $\mathbf{Z}$ 内恒有解而且只有一个解 $x=b-a$. 由此可知整数环有加法消去律: 若 $a+c=b+c$, 则 $a=b$. 两个非零整数的积不能等于零, 从而推出整数环还有乘法消去律: 若 $ac=bc$ 且 $c\neq 0$, 则 $a=b$.

下面引进整数环的 **序**, 即整数的大小. 对于任意整数 a,b, 规定

$$a\leq b \iff b-a\in \mathbf{N}.$$

若 $a\leq b$ 且 $a\neq b$, 则记成 $a<b$. $a\leq b$(或 $a<b$) 也可写成 $b\geq a$ (或 $b>a$). 整数的序有如下的性质:

1) $a<b, a=b, a>b$ 必有一而且只有一成立;
2) 若 $a\leq b$ 且 $b\leq c$, 则 $a\leq c$;
3) 若 $a\leq b$, 则 $a+c\leq b+c$, 对任意 $c\in \mathbf{Z}$;
4) 若 $a\leq b$ 且 $c>0$, 则 $ac\leq bc$.

自然数的序在整数环内仍然保持不变.

整数 a 的 **绝对值** $|a|$ 规定如下

$$|a|=\begin{cases} a, & 若a\geq 0,\\ -a, & 否则. \end{cases}$$

绝对值的性质有

$$|a|=0 \iff a=0,$$

$$|a+b|\leq |a|+|b|,$$

$$|ab|=|a|\cdot|b|.$$

下面来看整数的 **整除性**. 在整数环 $\mathbf{Z}$ 内已经知道方程 $a+x=b$ 恒有解, 但是方程 $ax=b(a\neq 0)$ 则不必有解. 为了使得方程 $ax=b(a\neq 0)$ 恒有解, 解决的方法就是仿照从自然数系构造整数环的方法将整数环扩充成有理数域. 这是在初等代数中早已解决了的问题. 这种构造方法将在第三章中推广到整环上去. 在本章中我们限制在整数环 $\mathbf{Z}$ 中研究方程 $ax=b$ 有解的条件, 这样将导出

整数环的整除性和同余式的理论. 在中小学已经知道判断上述方程是否有解的一个可行的方法就是带余除法. 从带余除法得到的结论就是

除法算式 *对任一对整数 $a,b,b\neq 0$, 存在一对整数 q 和 r 满足*

$$a=b\cdot q+r,\quad 0\leq r<|b|.$$

而且这样的 q 和 r 是唯一的. r 称为 a 被 b 除的 **余数**.

证明 当 $a\geq 0,b>0$ 时, 用 b 对 a 作带余除法, 可得到一个商数 q 和适合条件的余数 r. 我们在这里不打算给出正式的证明. a,b 的其余情况不难归结为上述情况. 下面证明 q,r 的唯一性. 设有两对 $q_i,r_i,i=1,2$ 使得

$$a=q_1b+r_1,\quad 0\leq r_1<|b|,$$
$$a=q_2b+r_2,\quad 0\leq r_2<|b|.$$

两式相减得

$$(q_2-q_1)b=r_1-r_2.$$

取绝对值

$$|q_2-q_1||b|=|r_1-r_2|.$$

假若 $r_1\neq r_2$, 则 $0<|r_1-r_2|<|b|$, 从而 $|q_2-q_1|\neq 0, |q_2-q_1|\cdot|b|<|b|$, 矛盾. 所以 $r_1=r_2$, 从而 $q_1=q_2$. □

除法算式是整除性理论的基础.

在除法算式中若 $r=0$, 则称 b **整除** a, 记作 $b|a$. 否则称作 b 不整除 a, 记作 $b\nmid a$.

对于整数 a,b, 若存在一个整数 c 使得 $a=bc$, 则称 b 是 a 的 **因子**, a 是 b 的 **倍数**. 从除法算式得到如下的

推论 *一个非零整数 b 是整数 a 的因子, 其充分必要条件是 b 整除 a.*

1 和 -1 是任何整数的因子. 每个整数是零的因子. 每个整数和它的负元素都是它自身的因子, 即 $\pm a|a$. 关于整除有下列基本性质:

1) 若 $a|b$ 且 $b|a$, 则 $a=b$ 或 $a=-b$. 此时 a,b 叫做 **相伴**.

2) 若 $a|b$ 且 $b|c$, 则 $a|c$.

3) 若 $c|a$ 且 $c|b$, 则 $c|ua+vb, u,v\in\mathbf{Z}$.

若整数 $c|a$ 且 $c|b$, 则 c 叫做整数 a,b 的 **公因子**. 设 d 是整数 a,b 的一个公因子, 若 a,b 的每个公因子也是 d 的因子, 则 d 叫做 a,b 的一个 **最大公因子**.

下面我们将证明任一对整数 a,b 都有最大公因子. 在证明存在之前, 先看一下 a,b 有多少最大公因子. 设 d_1,d_2 为整数 a,b 的两个最大公因子. 根据最大公因子的定义, 由于 d_1 是 a,b 的最大公因子, 有 $d_2|d_1$. 又因 d_2 也是 a,b 的

最大公因子，有 $d_1|d_2$, 所以 d_1, d_2 相伴. 因此任一对整数最多有一对相伴的最大公因子.

定理 2 任一对不全为零的整数 a, b 都有最大公因子，而且它可以表成 a, b 的一个组合 $ua + vb, u, v \in \mathbf{Z}$.

证明 考察 a, b 的一切组合的绝对值集合 $S = \{|xa + yb| \mid x, y \in \mathbf{Z}\}$. S 是自然数系的一个非空子集，而且 S 还包含有不为 0 的自然数. 根据 $\mathbf{N}$ 的良序性质，S 必然包含一个非零的最小自然数，记作 d. 于是 d 显然可表成 a, b 的组合 $d = ua + vb$. 首先证明 $d|a$ 且 $d|b$. 假若 $d \nmid a$. 用 d 对 a 作带余除法 $a = qd + r, 0 \le r < d$. 因 $d \nmid a, r > 0$. 于是

$$r = a - qd = a - q(ua + vb) = (1 - qu)a - qvb.$$

将有 $r \in S$. 但是 $0 < r < d$, 这与 d 的选取矛盾. 所以 $d|a$. 同理 $d|b$. 其次，证明 d 是 a, b 的最大公因子. 设 c 为 a, b 的任一公因子，则 $c|a$ 且 $c|b$, 从而 $c|d = ua + vb$, 所以 d 是 a, b 的一个最大公因子. □

综上所述可知任一对不全为零的整数 a, b, 恰有一对相伴的最大公因子，以后提到 a, b 的最大公因子时总是指大于 0 的那一个，并记作 (a, b). 计算 (a, b) 的一个有效的方法就是辗转相除法，这是大家所熟悉的，在这里不重复了.

如果两个不全为 0 的整数 a, b 的最大公因子为 1, 则 a, b 叫做**互素**.

定理 3 互素有如下性质：

1) 整数 a, b 互素的充要条件是 1 可以表成 a, b 的组合；

2) 若 $c|ab$ 且 $(c, a) = 1$, 则 $c|b$;

3) 若 $a|c$ 且 $b|c$ 且 $(a, b) = 1$, 则 $a \cdot b|c$;

4) 若 $(a, c) = 1, (b, c) = 1$, 则 $(a \cdot b, c) = 1$.

证明

1) 显然.

2) 因为 $(c, a) = 1$, 存在 $u, v \in \mathbf{Z}$ 使得 $uc + va = 1$. 两端乘以 $b, ucb + vab = b$. 由于 $c|cb$ 且 $c|ab$, 有 $c|b$.

3) 因为 $c|a$, c 可以写成 $c = ac_1$. 由于 $b|ac_1$ 且 $(b, a) = 1$, 根据 2), 有 $b|c_1$. 于是 $c_1 = bc_2$. 最后得 $c = abc_2$, 从而 $ab|c$.

4) 因为 $(a, c) = 1$, 存在 $u, v \in \mathbf{Z}$ 使得 $ua + vc = 1$. 因为 $(b, c) = 1$, 存在 $r, s \in \mathbf{Z}$ 使得 $rb + sc = 1$. 于是

$$1 = (ua + vc)(rb + sc) = urab + (usa + vrb + vsc)c,$$

根据 1), $(a \cdot b, c) = 1$. □

如果一个大于 1 的整数 p 除了 ± 1 和 $\pm p$ 外没有其它因子，则 p 叫做一个**素数**.

推论 设 p 为一素数，则

1) 对任一整数 a, 若 $p \nmid a$, 则 $(p,a)=1$;

2) 若 $p|ab$, 则 $p|a$ 或 $p|b$.

证明

1) 设 $d=(p,a)$, 因为 p 为一素数， d 只能是 p 或 1. 若为前者，则有 $p|a$, 与假设矛盾，所以 d 只能是 1, 即 $(p,a)=1$.

2) 设 $p|ab$, 若 $p \nmid a$. 由于 1) 有 $(p,a)=1$. 根据定理 3, 2) 得 $p|b$. □

最后证明

算术基本定理 每个大于 1 的整数 a 可以写成有限多个素数的乘积 $a = p_1p_2\cdots p_r$, 而且这些素因子按大小顺序排列后，写法只有一种.

证明 首先证明 a 可以分解成有限多个素数的乘积，对 a 作归纳法. 假设对所有整数 $a, 1<a<n$, a 可以写成有限多个素数的乘积，从而证明当 $a=n$ 时 a 也可以写成有限多个素数的乘积. 若 a 为素数，则 a 本身就是一种写法，设 a 不是素数，则 a 有一个因子 a_1, 使得 $1<a_1<a$, 于是 a 可以分解成 $a=a_1a_2$, 从而也有 $1<a_2<a$. 根据归纳法假设， a_1 和 a_2 分别可以分解成有限多个素因子的积. 因而 a 也可以分解成有限多个素因子的积. 其次证分解的唯一性. 设 a 有两种分解

$$a = p_1p_2\cdots p_r = q_1q_2\cdots q_s,$$

其中 p_i 和 q_j 都是素数. 求证 $r=s$ 且 q_j 在适当调换脚标后有 $q_i=p_i, i=1,2,\cdots,r$. 对 r 作归纳法. 当 $r=1, a=p_1$ 为素数，因而 $s=1, p_1=q_1$. 假设对 $r-1$ 分解是唯一的从而证明对 r 也是唯一的. 根据素数的性质，从 $p_1|a=q_1q_2\cdots q_s$, 可知 p_1 整除某个 q_i. 设 $p_1|q_1$. 于是 $q_1=p_1b$. 由于 q_1 也是素数，推出 $b=1, q_1=p_1$. 从上式两端消去 p_1 得 $p_2\cdots p_r=q_2\cdots q_s$. 根据归纳法假设有 $r-1=s-1$ 而且适当改换 q_i 的脚标后有 $q_i=p_i, i=2,\cdots,r$. 这就证明了 a 的分解是唯一的. □

在基本定理 a 的分解式中将相同的素因子归并写成幂的形式，于是就得到 a 的 **标准分解式**

$$a = p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t},\quad e_i\geq 1, p_i\neq p_j, i\neq j.$$

整除的条件也可以利用标准分解式来说明. 任给两个大于 1 的整数 a,b, 设

$p_1,\cdots,p_r$ 是 a 和 b 的全部不同的素因子. 于是 a,b 有分解式

$$a=p_1^{s_1}p_2^{s_2}\cdots p_r^{s_r},\quad s_i\geq 0,$$
$$b=p_1^{t_1}p_2^{t_2}\cdots p_r^{t_r},\quad t_i\geq 0.$$

容易证明 $a|b$ 的充要条件是 $s_i\leq t_i, i=1,2,\cdots,r$.

§4 同余式和同余方程

在整数环 $\mathbf{Z}$ 中我们引进一个基本的等价关系, 即同余概念. 它和整数的运算是相容的, 从而产生新的代数结构. 同余概念在代数中产生了广泛的影响.

定义 2 设 n 为一正整数, a,b 为任意整数. 如果 $n|(a-b)$, 则 a,b 叫做 **模 n 同余**, 记作

$$a\equiv b\ (\mathrm{mod}\ n),$$

n 叫做 **模数**. 否则, a,b 叫做 **模 n 非同余**, 记作 $a\not\equiv b\ (\mathrm{mod}\ n)$. 以下的讨论恒固定一个模数或几个模数.

容易证明 $a\equiv b\ (\mathrm{mod}\ n)$ 的充要条件是除法算式 $a=q_1n+r_1$ 和 $b=q_2n+r_2$ 有相同的余数 $r_1=r_2$.

同余概念最适宜于描写一种有限多个状态的周期现象. 例如计算某一天是星期几, 可以取 7 作模数. 计算一个整数是否是偶数, 可以取 2 作模数. 取 2 作模数, 余数 0 和 1 还可以描写电路的连接和断开. 同余概念和整数的运算是相容的, 表现在下列基本性质中. 模数固定时, $a\equiv b\ (\mathrm{mod}\ n)$ 可简写成 $a\equiv b$. 如果不写出模数, 表示是对同一个模数而言的.

1. 同余是一个等价关系.
2. 若 $a\equiv b, c\equiv d$, 则 $a\pm b\equiv b\pm d\ (\mathrm{mod}\ n)$.
3. 若 $a\equiv b, c\equiv d$, 则 $a\cdot c\equiv b\cdot d\ (\mathrm{mod}\ n)$.
4. 若 $ac\equiv bc\ (\mathrm{mod}\ n), (c,n)=1$, 则 $a\equiv b\ (\mathrm{mod}\ n)$.
5. 若 $a\equiv b\ (\mathrm{mod}\ n), m|n$, 则 $a\equiv b\ (\mathrm{mod}\ m)$.
6. 若 $a\equiv b\ (\mathrm{mod}\ n)$, 则 $(a,n)=(b,n)$.
7. 若 $a\equiv b\ (\mathrm{mod}\ n), d$ 为 a,b,n 的一个公因子, $a=da_1, b=db_1, n=dn_1$, 则 $a_1\equiv b_1\ (\mathrm{mod}\ n_1)$.

这些性质的证明都很容易, 请读者自己证明之.

例 1 $716\cdot 93$ 和 $543\cdot 93$ 模 61 是否同余? 假设 $716\cdot 93\equiv 543\cdot 93\ (\mathrm{mod}\ 61)$, 根据性质 4, 因 $(93,61)=1$, 有 $716\equiv 543\ (\mathrm{mod}\ 61)$. 但 $61\nmid(716-543)=173$, 所以 $716\cdot 93\not\equiv 543\cdot 93\ (\mathrm{mod}\ 61)$.

例 2 设复数 $\varepsilon=\cos\frac{2\pi}{17}+i\sin\frac{2\pi}{17}$. 计算 ε 的整数幂 ε^m 等于计算 ε^r, 其中 r 是 m 模 17 的余数, $0\le r<17$.

对于一个给定的模数 n, 全体整数按模 n 同余分成一些等价类, 此时的等价类叫做 **整数模 n 的剩余类**, 含整数 a 的剩余类记作 $\overline{a}$, 剩余类 $\overline{a}$ 的任一个元素叫做 $\overline{a}$ 的一个代表. 在每个剩余类中任取一个代表 r_i, 由这些代表组成的集合叫做整数模 n 的一个 **完全剩余代表系**. 整数模 n 的一个完全剩余代表系 S 也可以这样来刻画: 1) 每个整数和 S 中一个元素模 n 同余, 2) S 中元素两两互不同余. 根据除法算式可知, 集合 $S=\{0,1,2,\cdots,n-1\}$ 是模 n 的一个完全剩余代表系.

由模 n 的剩余类组成的商集记作 $\mathbf{Z}/(n)$. 在 $\mathbf{Z}/(n)$ 中可以定义加法和乘法如下:

$$\overline{a}+\overline{b}=\overline{a+b},$$
$$\overline{a}\cdot\overline{b}=\overline{a\cdot b}.$$

根据同余式的性质, 定义与代表的取法无关而且加法和乘法还满足结合律、交换律和分配律, 加法有零元素 $\overline{0}$, 每个 $\overline{a}$ 有负元素 $\overline{-a}:\overline{a}+(\overline{-a})=\overline{0}$. $\mathbf{Z}/(n)$ 叫做 **整数模 n 的环**.

这一节剩下的部分来讨论一次同余方程和方程组. 同余式

$$ax\equiv b\ (\mathrm{mod}\ n),\quad a\not\equiv 0\ (\mathrm{mod}\ n)$$

是含有一个未知量 x 的一次式, 叫做 **一次同余方程**. 若 $x=c\in\mathbf{Z}$ 代入上方程使两边同余, 则 c 叫做上方程的一个 **解**. 上方程的两个解 c_1,c_2 看作相同当而且仅当 $c_1\equiv c_2\ (\mathrm{mod}\ n)$.

定理 4 *设 $(a,n)=1$, 则一次同余方程*

$$ax\equiv b\ (\mathrm{mod}\ n)$$

有解而且只有一个解.

证明 由于 $(a,n)=1$, 存在整数 u,v 使得 $ua+vn=1$. 两边乘 b, $uba+vbn=b$, 令 $ub=c$, 于是 $ca\equiv uba+vbn\equiv b\ (\mathrm{mod}\ n)$, $x\equiv c$ 为其一解. 其次, 令 c_1,c_2 为任意两个解, 于是

$$ac_1\equiv b\ (\mathrm{mod}\ n),$$
$$ac_2\equiv b\ (\mathrm{mod}\ n).$$

相减得 $a(c_1-c_2)\equiv 0\ (\mathrm{mod}\ n)$, 由于 $(a,n)=1$, 根据同余的性质 4, 有 $c_1\equiv c_2\ (\mathrm{mod}\ n)$, c_1,c_2 为同一解. □

考虑下列 **一次同余方程组**

$$\begin{cases} x \equiv b_1 \pmod{n_1}, \\ x \equiv b_2 \pmod{n_2}, \\ \cdots\cdots\cdots\cdots\cdots \\ x \equiv b_r \pmod{n_r}. \end{cases} \tag{1}$$

其中 $n_1, n_2, \cdots, n_r$ 为大于 1 的整数，两两互素， $b_1, b_2, \cdots, b_r$ 是任意给定的整数．如果 $x = c \in \mathbf{Z}$ 代入上方程组使得同余式同时都成立，则 c 叫做方程组 (1) 的一个解．上方程组的两个解 c_1 和 c_2 看作相同当而且仅当

$$c_1 \equiv c_2 \pmod{\prod_{i=1}^{r} n_i}.$$

定理 5 **(孙子定理)** 设一次同余方程组 (1) 中大于 1 的整数 $n_1, n_2, \cdots, n_r$ 两两互素， $b_1, b_2, \cdots, b_r$ 是任意给定的整数，则 (1) 有解而且只有一解．

证明 这里只证明 $r = 2$ 的情况，读者可以应用数学归纳法去证明一般情况．设 $r = 2$, 由于 $(n_1, n_2) = 1$, 存在一对整数 u_1, u_2 使得 $u_1 n_1 + u_2 n_2 = 1$. 令 $e_2 = u_1 n_1, e_1 = u_2 n_2$. 于是 $e_i \equiv 1 \pmod{n_i}, i = 1, 2$, 而 $e_i \equiv 0 \pmod{n_j}, i \neq j$. 取 $c = b_1 e_1 + b_2 e_2$, 则 c 为方程组 (1) 的解．其次证明解的唯一性，设 c_1, c_2 为任意两解，于是

$$\begin{aligned} c_1 \equiv b_1, \ c_2 \equiv b_1 \pmod{n_1}, \\ c_1 \equiv b_2, \ c_2 \equiv b_2 \pmod{n_2}. \end{aligned}$$

同余式相减得

$$\begin{aligned} c_1 - c_2 \equiv 0 \pmod{n_1}, \\ c_1 - c_2 \equiv 0 \pmod{n_2}. \end{aligned}$$

由于 $(n_1, n_2) = 1$, 根据互素性质 3) $c_1 - c_2 \equiv 0 \pmod{n_1 n_2}$, 所以 c_1, c_2 为同一解． □

孙子定理在国际上叫做中国剩余定理．

§5 欧拉函数和欧拉 - 费马定理

首先介绍数论中一个重要的函数即欧拉函数．

设 n 为一正整数，在 $0, 1, 2, \cdots, n-1$ 中与 n 互素的整数的个数记作 $\varphi(n)$, 叫做 **欧拉函数**．由同余性质 6 知道， $\varphi(n)$ 也就是那些模 n 的剩余类的个数，这些剩余类是由与 n 互素的整数组成的．从这些剩余类取出的代表所组成的集合叫做 **模 n 的既约剩余代表系**．一个既约剩余代表系 T 也可以这样来刻画：

1) 任一个与 n 互素的整数必与 T 中一个数模 n 同余，而且 2) T 中整数与 n 互素而且模 n 两两不同余.

设 $r_1, r_2, \cdots, r_N, N = \varphi(n)$, 为模 n 的一个既约剩余代表系，$(a, n) = 1$, 则 $ar_1, ar_2, \cdots, ar_N$ 仍是模 n 的一个既约剩余代表系. 这是因为，首先根据互素性质 4) 和同余性质 4, $ar_1, ar_2, \cdots, ar_N$ 与 n 互素而且两两互不同余 (mod n). 其次，每个 ar_i 和某一个 r_{a_i} $(1 \le a_i \le N)$ 同余，而且当 $i \ne j$ 有 $a_i \ne a_j$, 于是 $ar_i \mapsto r_{a_i}$ 是一个单射，因而是一个满射. $a_1, a_2, \cdots, a_N$ 是 $1, 2, \cdots, N$ 的一个排列. 由于每个与 n 互素的整数 b 必与某个 r_{a_i} 同余，由上可知 b 必与 ar_i 同余. 所以 $ar_1, ar_2, \cdots, ar_N$ 是模 n 的既约剩余代表系.

定理 6 **(欧拉 - 费马(Fermat))** 设 $(a, n) = 1, N = \varphi(n)$, 则

$$a^N \equiv 1 \pmod{n}.$$

证明 取模 n 的一个既约剩余代表系 $r_1, r_2, \cdots, r_N$. 由于 $(a, n) = 1, ar_1, ar_2, \cdots, ar_N$ 也是一个既约剩余代表系，而且 $ar_i \equiv r_{a_i} \pmod{n}, a_1, a_2, \cdots, a_N$ 是 $1, 2, \cdots, N$ 的一个排列. 这 N 个同余式连乘得

$$\prod_{i=1}^{N} ar_i \equiv \prod_{i=1}^{N} r_{a_i} = \prod_{i=1}^{N} r_i \pmod{n},$$
$$a^N \prod r_i \equiv \prod r_i \pmod{n},$$

根据互素性质 4), $\prod r_i$ 与 n 互素, 根据同余式性质 4, 消去 $\prod r_i$ 得 $a^N \equiv 1 \pmod{n}$. □

定理 6 的特殊情况是，$n = p$ 为一素数，$\varphi(p) = p - 1$. $(a, p) = 1$ 即 $p \nmid a$, 于是

$$a^{p-1} \equiv 1 \pmod{p}.$$

这就是费马定理. 费马定理也可写成：对任意素数 p 和任意整数 a, 恒有

$$a^p \equiv a \pmod{p}.$$

在这里顺便介绍一下指数的概念. 设 a, n 为互素的一对整数，$n \ge 1$, 则存在一个最小正整数 m 使得

$$a^m \equiv 1 \pmod{n},$$

m 叫做 a 模 n 的 **指数**. 指数的存在由欧拉 - 费马定理得到保证. 因为使 $a^k \equiv 1 \pmod{n}$ 的正整数 k 存在，$\varphi(n)$ 就是一个. k 的存在也可直接看出. 因为

$a, a^2, a^3, \cdots$ 中必有两个同余的，设 $a^j \equiv a^i \pmod{n}, j > i$, 消去 a^i 使 $a^{j-i} \equiv 1 \pmod{n}$. 应用除法算式可以证明指数的一个基本性质:

$a^k \equiv 1 \pmod{n} \iff m|k, m$ 为 $a \bmod n$ 的指数. 特别地，指数 $m|\varphi(n)$.

例 2 mod 17 的指数为 8, 3 mod 17 的指数为 $16 = \varphi(17)$. 计算 $3^{157} \bmod 17$, 可应用指数.

首先，$157 \equiv 13 \pmod{16}, 3^{157} \equiv 3^{13} \pmod{17}$, 而 $3^{13} \equiv 3^8 \cdot 3^5 \equiv -3^5 \equiv -5 \pmod{17}$.

下面我们来计算欧拉函数.

引理 1 p 为素数，$\varphi(p^m) = p^m\left(1 - \dfrac{1}{p}\right)$, $m \geq 1$.

证明 因为在 $S = \{0, 1, 2, \cdots, p^m - 1\}$ 中除去 p 的倍数，剩下的都与 p 互素，而 S 中 p 的倍数恰好有 $\dfrac{p^m}{p}$ 个，因此 S 中与 p 互素的整数的个数为 $p^m - p^{m-1}$. □

引理 2 设 $n = n_1 \cdot n_2$, $(n_1, n_2) = 1, n_i \geq 1$, 则

$$\varphi(n) = \varphi(n_1) \cdot \varphi(n_2).$$

证明 $\varphi(n_i)$ 简记作 $N_i, i = 1, 2$. 设 $r_1, \cdots, r_{N_1}$ 和 $s_1, \cdots, s_{N_2}$ 分别为模 n_1 和模 n_2 的既约剩余代表系. 根据孙子定理, 存在整数 $t_{ij}, i = 1, \cdots, N_1, j = 1, \cdots, N_2$ 使得

$$t_{ij} \equiv r_i \pmod{n_1},$$
$$t_{ij} \equiv s_j \pmod{n_2}.$$

证明 t_{ij} 为模 $n_1 n_2$ 的一个既约剩余代表系. 首先, 由于 $(r_i, n_1) = 1$, 有 $(t_{ij}, n_1) = 1$. 由于 $(s_j, n_2) = 1$, 有 $(t_{ij}, n_2) = 1$. 因而 $(t_{ij}, n_1 n_2) = 1$. 其次 t_{ij} 互不同余. 假若 $t_{ij} \equiv t_{kl} \pmod{n_1 n_2}$, 一方面有 $t_{ij} \equiv t_{kl} \pmod{n_1}$, 它化为 $r_i \equiv r_k \pmod{n_1}$, 从而 $i = k$, 另一方面有 $t_{ij} \equiv t_{kl} \pmod{n_2}$, 它化为 $s_j \equiv s_l \pmod{n_2}$, 从而 $j = l$. 所以 t_{ij} 互不同余 $(\bmod\ n_1 n_2)$. 最后设 a 为任一与 n 互素的整数，根据 r_i 和 s_j 的定义，存在 r_i 和 s_j 使得 $a \equiv r_i \pmod{n_1}, a \equiv s_j \pmod{n_2}$, 于是根据孙子定理有 $a \equiv t_{ij} \pmod{n}$. 所以 t_{ij} 是模 n 的一个既约剩余代表系. 这证明了 $\varphi(n) = \varphi(n_1) \cdot \varphi(n_2)$. □

定理 7 设 $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}, p_1, p_2, \cdots, p_r$ 为不同素数，$e_i \geq 1$, 则

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

应用引理 1 和引理 2 对 r 作归纳法即得.

最后证明欧拉函数的一个性质

$$\sum_{d|n}\varphi(d)=n.$$

设 $S=\{0,1,\cdots,n-1\}$, 对每个 $d|n$, 令 $S_d=\{x\in S\,|\,(x,n)=d\}$. 显然 $S=\bigcup\limits_{d|n}S_d$ 是 S 的一个划分. 其次, 映射

$$\eta: x\mapsto \frac{x}{d},\ x\in S_d$$

是 S_d 到 $S\left(\frac{n}{d}\right)=\left\{0,1,2,\cdots,\frac{n}{d}-1\right\}$ 的一个单射. 而且象集 $\eta(S_d)$ 恰好是 $S\left(\frac{n}{d}\right)$ 中与 $\frac{n}{d}$ 互素的整数全体. 所以 $|S_d|=\varphi\left(\frac{n}{d}\right)$, 由此得

$$n=\sum_{d|n}|S_d|=\sum_{d|n}\varphi\left(\frac{n}{d}\right),$$

当 d 走遍 n 的因子时, $\frac{n}{d}$ 刚好走遍 n 的因子, 所以

$$\sum_{d|n}\varphi\left(\frac{n}{d}\right)=\sum_{d|n}\varphi(d).$$

§6 偏序集合

集合 S 上的一个关系, 记作 $\leq$, 叫做一个 **偏序**, 如果 $\leq$ 满足

1) 反身性 $a\leq a$ 对所有 $a\in S$;

2) 反对称性 若 $a\leq b$ 且 $b\leq a$, 则 $a=b$;

3) 传递性 若 $a\leq b$ 且 $b\leq c$, 则 $a\leq c$.

一个具有偏序的集合叫做 **偏序集合**, 如果集合 S 上一个偏序 $\leq$ 对于任意 $a,b\in S$ 恒有 $a\leq b$ 或 $b\leq a$, 则 $\leq$ 叫做一个 **全序**. 偏序集合的元素 a,b 叫做 **可比较的**, 如果 $a\leq b$ 和 $b\leq a$ 有一成立. 如果一个偏序集合 S 的一个子集 A 的任一对元素都是可比较的, 则 A 叫做 S 的一个 **链**.

例 1 设 X 为一集合. X 的幂集 $P(X)$ 按 X 的包含关系构成一个偏序集合, $P(X)$ 为一个链当而且仅当 X 为空集或只含一个元素.

例 2 自然数系 $\mathbf{N}$ 按小于等于号 $\leq$ 是一个全序集合.

例 3 自然数系 $\mathbf{N}$ 的整除关系 $a|b$ 记成 $a\leq b$, 就是一个偏序.

设 S 为一个偏序集合. 元素 $a\in S$ 叫做 S 的一个 **极小元素**, 如果 S 没有元素 x 使得 $x<a$(即 $x\leq a,x\neq a$), 或者说从 $x\leq a$ 推出 $x=a$. 仿此, 元素 $a\in S$

叫做 S 的一个 **极大元素**, 如果不存在 $x \in S$ 使得 $a < x$, 或者说如果从 $a \leq x$ 可推出 $a = x$. 若 S 有极大 (小) 元素 a, 并不要求 a 与 S 的所有元素可以比较.

例 4 令 $N_1 = \mathbf{N} - \{0, 1\}$, N_1 按整除关系是一偏序集合, 此时每个素数是 N_1 的极小元素, N_1 没有极大元素.

设 A 为偏序集合 S 的一个子集, 元素 $a \in S$ 叫做 A 的一个 **下界**, 如果对所有的 $x \in A$ 都有 $a \leq x$. 类似, 元素 $a \in S$ 叫做 A 的一个 **上界**, 如果对所有 $x \in A$ 都有 $x \leq a$. A 可以没有下界或有多个下界. 若 A 有下界, 也不要求它属于 A, 对上界也如此. 在例 2 中令 $A = \{2k \,|\, k \in \mathbf{N}\}$, A 没有上界但有下界 0 且 $0 \in A$. 在例 3 中令 $B = \{2k+1 \,|\, k \in \mathbf{N}\}$, B 有一上界 0, 但 $0 \notin B$.

设 S 为一个偏序集合, A 为一个子集, 如果 A 有一个下界 a 而且 $a \in A$, 则 a 叫做 A 的一个 **最小元素**. 类似地, 如果 A 有一个上界 a 而且 $a \in A$, 则 a 叫做 A 的一个 **最大元素**. A 可以没有最小 (大) 元素, 如果 A 有最小 (大) 元素, 则它是唯一的.

在例 1 中空集是 $P(X)$ 的最小元素, X 是 $P(X)$ 的最大元素. 在例 2 中 0 是 $\mathbf{N}$ 的最小元素, $\mathbf{N}$ 没有最大元素. 在例 3 中, 1 是 $\mathbf{N}$ 的最小元素. 0 是 $\mathbf{N}$ 的最大元素.

§7 选择公理、佐恩引理和良序定理

在代数中有一类定理是断言某种对象的存在性, 这种对象属于一定的集合而且具有特定的性质. 如果赋予集合以适当的偏序, 那么特定的性质就表现为一种极值性质. 从而断言某种对象的存在就转变成断言一个偏序集合的极大元素的存在. 例如我们断言一个域上线性空间 V 的基的存在, 我们可以考虑 V 中一切线性无关向量组 (包含的向量个数有限或无限) 作元素构成的集 S. 按向量组的包含关系规定 S 的偏序, 于是 V 的基的存在问题就转变为偏序集 S 有无极大元素的问题. 为了证明这一类存在定理, 我们介绍几个广泛应用的极大原理和良序定理. 它们都是从选择公理演变而来, 并且与选择公理等价的. 选择公理是首先由策梅洛 (Zermelo) 于 1904 年提出来的.

选择公理 *设 $T = \{A_\alpha \,|\, \alpha \in I\}$ 为一族非空集合 $A_\alpha, \alpha \in I$ (I 为指标集), 组成的非空集, 则存在一个 T 上的函数 f 使得对所有 $\alpha \in I$ 恒有 $f(A_\alpha) \in A_\alpha$.*

f 叫做 T 上的一个 **选择函数**, 选择函数的存在作为公理提出来意味着存在某种规律使得可以从每个 $A_\alpha, \alpha \in I$, 同时地挑出一个元素. 当 $A_\alpha, \alpha \in I$ 都是同一个可数无限集 S 的子集时, 先将 S 的元素用自然数编号, 然后定义函数 f 在 A_α 上的值为 A_α 中有最小编号的元素, 于是 f 就是 $\{A_\alpha \,|\, \alpha \in I\}$ 上的一个选择函数. 当指标集合 I 为有限或可数无限时, 根据自然数的递归定理可以证明选

择函数的存在. 一般情况, 选择公理是不能证明的.

集合 S 上的一个偏序叫做**良序的**, 如果 S 的每个非空子集都有最小元素. 具有良序的集合叫做**良序集合**. 良序必然是全序的. 自然数集合按通常的小于等于 $\leq$ 是一个良序集合. 空集看作良序集合. 策梅洛应用选择公理证明了著名的

良序定理 *每个集合都存在一个良序.*

限于篇幅, 在这里不打算给出证明.

反之, 从良序定理容易推出选择公理.

良序定理的重要性在于自然数集合的数学归纳法原理可以推广到良序集合上去, 从而得到超限归纳法原理. 设 S 是一个良序集合, 对于任一 $a \in S$, 子集 $S(a) = \{x \in S \mid x < a\}$ 叫做 S 的一个**前段**.

超限归纳法原理 *设 S 是任一个良序集合, A 为 S 的任一个子集. 如果对于任一元素 $a \in S$ 从 S 的前段 $S(a)$ 包含在 A 内推出 $a \in A$, 则 $A = S$.(S 的最小元素 a_0 必然属于 A, 因为 $S(a_0) = \emptyset \in A$.)*

证明 完全与第二数学归纳法的证明类似. □

假设有一个性质或命题 $E(a)$ 与一个良序集合 S 的每个元素 a 相联系, 可以应用超限归纳法原理证明性质或命题 $E(a)$ 对所有 $a \in S$ 都成立. 就是说, 如果我们能够证明, 对于每个元素 $a \in S$ 从 $E(x)$ 对所有 $x \in S(a)$ 都成立推出 $E(a)$ 也成立, 则根据超限归纳法原理, $E(x)$ 对一切 $x \in S$ 都成立. 这就是超限归纳证明法.

还有超限归纳构造法, 不打算在这里叙述.

与选择公理等价的还有一个非常重要的极大原理, 也就是佐恩 (Zorn) 引理. 它和良序定理比较, 应用起来方便得多, 因而得到广泛的应用.

极大原理 *设 T 为由集合 S 的若干子集作元素组成的非空集合, T 按包含关系成一个偏序集. 如果 T 的每个链都有一个上界, 则 T 有一个极大元素.*

将集合 T 抽象化, 极大原理可叙述成

佐恩引理 *若一个偏序集 S 的每个链都有上界, 则 S 有一个极大元素.*

现在我们来说明, 佐恩引理可以换写成极大原理的形式, 因而这两者是等价的. 存在 S 到 S 的幂集 $P(S)$ 的一个映射 η: 对于每个 $a \in S$, 规定 $\eta(a) = \{x \in S \mid x \leq a\}$. 设 $a, b \in S, a \leq b$, 则根据偏序的传递性, 由 $x \in \eta(a)$ 有 $x \leq a$, 从而 $x \leq b, x \in \eta(b)$. 因此有 $\eta(a) \subset \eta(b)$. 反之, 从 $\eta(a) \subset \eta(b)$ 也可以推出 $a \leq b$. 因此, $\eta(a) = \eta(b) \iff a = b$. 所以 η 是 S 到 $P(S)$ 的一个单射而且保持偏序关系. 于是 $T = \eta(S)$ 是一个与 S 成一一对应, 保持偏序关系而且满足极大原理中的假设的偏序集合.

限于篇幅，上面列举的与选择公理等价的几个定理，它们的等价性不加证明[1].

最后我们应用佐恩引理来证明数域上线性空间 V 的基的存在. V 的一个非空向量组 A(包含向量的个数有限或无限) 叫做线性无关的，如果 A 的每个非空有限子集都是线性无关的. V 中一切线性无关的向量组作元素构成的集合 S 按包含关系成一偏序集. 设 $T=\{A_a \mid a\in I\}$ 为 S 的一个链，求证并集 $A=\bigcup\limits_{a\in I} A_a$ 也是一个线性无关的向量组. 设 $A_1=\{a_1,\cdots,a_r\}$ 是 A 的一个有限子集，于是每个 a_i 必包含在某一个 A_{a_i} $(a_i\in I)$ 内，由于 T 是一个链， $A_{a_1},\cdots,A_{a_r}$ 又包含在某一个 A_a $(a\in I)$ 内. 于是 $A_1\subset A_a$, 因而 A_1 是线性无关的向量组. 所以 A 是一个线性无关的向量组. 因而 $A\in S$. 显然 A 是 T 的一个上界. 根据佐恩引理的第一种形式， S 有一个极大元素 M. 根据 M 的极大性，可证向量组 M 就是 V 的基. 因为否则将存在一个向量 $b\in V$ 使得 b 不能表成 M 中任何有限向量组的线性组合. 读者自己证明 $B=M\cup\{b\}$ 是一个线性无关的向量组，因而 $B\in S$. 显然 $M\subset B$ 但 $M\neq B$, 这与 M 的极大性矛盾.

习 题

1. 设 X 与 Y 为两个集合，又设映射 $f:X\to Y$ 与 $g:Y\to X$. 如果 $g\cdot f=1_X$, 1_X 表示 X 的恒等映射，则称 g 为 f 的一个左逆. 如果 $f\cdot g=1_Y$, 则 g 叫做 f 的右逆. 如果 g 同时是 f 的左逆和右逆，则称 g 为 f 的一个逆. 证明:

(i) f 有左逆当而且仅当 f 是单射.

(ii) f 有右逆当而且仅当 f 是满射.

(iii) 如果 f 有左逆 g, 同时又有右逆 h, 则 $g=h$.

(iv) f 有逆当而且仅当 f 是一个一一对应.

(v) 如果 f 有逆，则 f 的逆是唯一的. f 的逆记作 f^{-1}.

(vi) 若 f 有逆，则 $(f^{-1})^{-1}=f$.

2. 举例说明，一个非空集合 S 上的等价关系的三条公理是独立的.

3. 整数集合 $\mathbf{Z}$ 上，存在映射 $f:\mathbf{Z}\to\mathbf{Z}$ 使得 f 有左 (右) 逆但无右 (左) 逆.

4. 试判断反身性、对称性和传递性对下列二元关系是否成立?

(i) 实数系 $\mathbf{R}$. $x-y$ 为 2π 的整数倍.

(ii) $\mathbf{R}$, $x\geq y$.

(iii) $\mathbf{R}$, $x>y$.

(iv) S 是仅含一个元素的集， $x>y$.

---

[1]有关证明读者可参看范德瓦尔登著《代数学 I》(丁石孙、曾肯成、郝锕新译，科学出版社， 1963) 第一章 §7 和 §8, 或库洛什著《一般代数学讲义》(刘绍学译，上海科技出版社, 1964).

5. 试判断反身性、对称性和传递性对下列二元关系是否成立?

(i) $\mathbf{R}, |x-y|=1$.

(ii) $\mathbf{R}, |x-y|\le 1$.

(iii) $\mathbf{R}, x-y=1$.

(iv) $\mathbf{R}, x+y=1$.

6. 证明自然数系的加法和乘法分别满足结合律和交换律.

7. 证明自然数系的乘法对加法的分配律成立.

8. 证明自然数系的乘法消去律成立, 即如果 $ax=ay, a\neq 0$, 则 $x=y$.

9. 在欧几里得平面上, 用 S 表示一切有方向的线段 PQ(起点 P, 终点 Q) 作成的集合. 请在 S 上给出一个等价关系 $\sim$ 使得商集成为平面上的向量集合.

10. 设 X, Y, Z 为任意集合, 又设 $\eta: X\to Y$, $\phi_i: Y\to Z$, $i=1,2$. 证明: "如果 $\phi_1\eta=\phi_2\eta$, 则 $\phi_1=\phi_2$" 对任意 ϕ_1,ϕ_2 都成立的充要条件是 η 是个满射.

11. 设 $\psi_i: X\to Y$, $i=1,2$, $\eta: Y\to Z$. 证明: "如果 $\eta\psi_1=\eta\psi_2$, 则 $\psi_1=\psi_2$" 对任意 ψ_1,ψ_2 都成立的充要条件是 η 是一个单射.

12. 证明: 在自然数系 $\mathbf{N}$ 中, 如果 $a\ge b, c\ge d$, 则 $a+c\ge b+d$ 而且 $ac\ge bd$.

13. 设 a 为一个非零整数, $m>n>0$, $m,n\in\mathbf{Z}$. 证明 $(a^{2^m}+1, a^{2^n}+1)=1$ 或 2. 从而证明有无穷多个素数. (波利亚 (G. Polya))

14. 定义在正整数集合 $\mathbf{Z}^+$ 上的**默比乌斯 (Möbius) 函数** $\mu(n)$ 规定如下:

(i) $\mu(1)=1$;

(ii) $\mu(n)=0$, 若 n 含有平方因子;

(iii) $\mu(n)=(-1)^r$, 若 $n=p_1p_2\cdots p_r$, p_i 为不同的素数.

证明: 对于正整数 $n>1$, 恒有

$$\sum_{d|n}\mu(d)=0.$$

15. 应用定理 7, 证明欧拉函数 $\varphi(n)$ 可写成

$$\varphi(n)=n\sum_{d|n}\frac{\mu(d)}{d}.$$

16. 设 p 为一素数, 证明威尔逊 (Wilson) 定理

$$(p-1)!\equiv -1 \pmod p.$$

17. 定义在整数 $\mathbf{Z}$ 上的函数 $f(n)$ 如果满足

$$f(n)\cdot f(m)=f(nm),$$

则 $f(n)$ 叫做乘性函数. 证明: 若 $f(n)$ 是一个乘性函数, 则 $g(n)=\sum_{d|n}f(d)$ 也是一个乘性函数.

18. 证明: 若 $f(n)$ 是一个乘性函数, 则 $h(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)f(d)$ 也是一个乘性函数.

19. (默比乌斯反演定理) 设 $f(n)$ 是定义在正整数集 $\mathbf{Z}^+$ 上的复值函数. 令 $F(n) = \sum_{d|n} f(d)$. 证明

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

20. 应用默比乌斯反演公式和欧拉函数 $\varphi(n)$ 的一个性质 $\sum_{d|n} \varphi(d) = n$, 来直接证明习题 15 的公式. 然后重新导出定理 7 的公式.

21. 证明

$$\sum_{\substack{1 \le r \le n \\ (r,n)=1}} r = \frac{1}{2} n \cdot \varphi(n).$$

22. 证明有无穷多个素数模 6 同余 -1.

23. 解同余方程

$$27x \equiv 25 \pmod{31}.$$

24. 解同余方程组

$$\begin{cases} x \equiv 2 \pmod{5}, \\ x \equiv 1 \pmod{7}, \\ x \equiv 5 \pmod{11}. \end{cases}$$

25. 将正整数 n 写成十进制 $n = a_1 a_2 \cdots a_r$, $1 \le a_1 \le 9, 0 \le a_i \le 9$, $i = 2, \cdots, r$. 证明:

(i) $n \equiv 0 \pmod{3} \iff \sum_{i=1}^{r} a_i \equiv 0 \pmod{3}$;

(ii) $n \equiv 0 \pmod{9} \iff \sum_{i=1}^{r} a_i \equiv 0 \pmod{9}$;

(iii) $n \equiv 0 \pmod{11} \iff \sum_{i=1}^{r} (-1)^i a_i \equiv 0 \pmod{11}$.

26. 设 p 为一素数, $r \ge 1$. 则每个整数 n, $0 \le n < p^r$ 可以唯一地与下列数之一模 p^r 同余:

$$a_0 + a_1 p + \cdots + a_{r-1} p^{r-1}, \ 0 \le a_i < p.$$

27. 设 p 为一素数, n 为一正整数.

(i) $x^2 \equiv 1 \pmod{p^r}$, $r \ge 1$, 有多少解? 并求解.

(ii) $x^2 \equiv 1 \pmod{n}$ 有多少解?

第一章　代数基本概念

§1　代数运算

从历史上看，在相当长的一段时间中，数及其四则运算一直是代数研究的主要对象．自 19 世纪以来，随着数学的发展，也就是随着人类认识的不断深化，运算的概念以及可以进行运算的对象大大超出了数的范围．就以我们已讨论过的对象而言，除去数以外，就还有多项式、函数、向量、矩阵、变换等，它们都可以进行运算，代数主要就是研究它们在运算下的性质．我们看到，虽然这些对象不同，它们之间各种运算的定义办法也不同，但是这些运算却有许多共同的性质．在这些问题研究的基础上，人们逐渐形成了一些抽象的概念．由于这些概念概括了许多重要的具体对象的共同性质，所以它们不但在代数中，而且在现代数学的理论与应用中都具有基本的重要性．本章就是介绍群、环与域这三个基本的代数概念，当然介绍只是初步的．

为了给出这些抽象概念的定义，我们首先需要给出一般的代数运算的定义．

定义 1　设 A 是一非空集合．任意一个由 $A\times A$ 到 A 的映射就称为定义在 A 上的一个 **代数运算**．

按映射的定义，所谓由 $A\times A$ 到 A 的映射就是指一个法则，它使 A 中任意两个元素 (这两个元素可以相同) 都有 A 中一个元素与它们对应．容易看到，这样定义的代数运算是一个极其广泛的概念，它的确把我们过去碰到过的运算的大部分包括在内．例如通常数的加法就是映射 $(a,b)\mapsto a+b$，矩阵的乘法就是映射 $(A,B)\mapsto AB$．当所考虑的集合是全体实数 $\mathbf{R}$ 时，这里所说的代数运算也就是通常的二元函数 $f(x,y)$，显然，$x+y$ 与 xy 都是特殊的二元函数．在这个定义下，对于实数 $\mathbf{R}$ 来说，映射 $(x,y)\mapsto x$，$(x,y)\mapsto 0$，$(x,y)\mapsto x+y^2$ 等都可以被认为是代数运算．虽然我们可以举出各式各样代数运算的例子，但是以下我们要讨论的总是那些具有适当性质的代数运算．

应当看到，在这个定义下，以前有些运算如向量的数量乘法与向量的内积就不是代数运算，因为在它们的定义中都涉及到两个集合．这些运算如何抽象化以后再另作处理．

§2　群的定义和简单性质

我们首先介绍群的概念．

定义 2　设 G 是一个非空集合．如果在 G 上定义了一个代数运算，称为乘法，记作 ab (或称为加法，记作 $a+b$)，而且它适合以下条件，那么 G 称为一个

群：

1) 对于 G 中任意元素 a, b, c 有

$$a(bc) = (ab)c \qquad \text{(结合律)};$$

2) 在 G 中有一个元素 e, 它对 G 中任意元素 a 有

$$ea = a;$$

3) 对于 G 中任一元素 a 都存在 G 中一个元素 b 使

$$ba = e.$$

下面看几个例子.

例 1 全体非零实数 $\mathbf{R}^*$ 对于通常的乘法成一个群; 全体正实数 $\mathbf{R}^+$ 对于通常的乘法也成一个群.

例 2 设 n 是一正整数, 全体 n 次单位根 (即方程 $x^n = 1$ 的 n 个根) 对于复数的乘法成一个群, 这个群记为 U_n; 特别地, 当 $n = 2$ 时, $U_2 = \{\pm 1\}$.

例 3 全体整数 $\mathbf{Z}$ 对于通常的加法成一个群; 同样, 全体有理数 $\mathbf{Q}$, 全体实数 $\mathbf{R}$, 全体复数 $\mathbf{C}$ 对加法也都是群.

例 4 设 V 是数域 P 上一线性空间. V 的全体可逆线性变换对于变换的乘法成一个群; 当 V 是一欧几里得空间时, V 的全体正交变换对于乘法也组成一个群.

例 5 元素在数域 P 中全体 n 级可逆矩阵对于矩阵的乘法成一个群, 这个群记为 $GL_n(P)$, 称为 n 级 **一般线性群**; $GL_n(P)$ 中全体行列式为 1 的矩阵对于矩阵乘法也成一个群, 这个群记为 $SL_n(P)$, 称为 **特殊线性群**.

从以上的例子可以看出, 群的概念确实概括了不少重要的对象的共同特征. 这里应该注意, 在群的定义中重要的是有一个代数运算, 至于这个代数运算叫什么名称以及用什么符号来代表是无关紧要的, 只有在具体的例子中它才有具体的含义. 在一般的讨论中, 我们不过把它叫做乘法而已.

现在根据群的定义我们来推导群 G 的一些基本性质.

1. 如果 $ba = e$, 则 $ab = e$.

证明 根据 3), 对于元素 b 有 $c \in G$ 使

$$cb = e.$$

于是

$$a = ea = (cb)a = c(ba) = ce,$$

两边用 b 右乘，得

$$ab = (ce)b = c(eb) = cb = e. \quad \square$$

2. 如果对所有的 $a \in G$ 有 $ea = a$, 那么也有 $ae = a$, 对所有的 $a \in G$.

证明 取 $b \in G$ 使 $ba = e$. 我们知道， $ab = e$. 于是

$$a = ea = (ab)a = a(ba) = ae. \quad \square$$

3. G 中有唯一的元素 e 具有性质

$$ea = ae = a, \text{ 对所有的 } a \in G.$$

证明 假设有 $e_1, e_2 \in G$, 它们都具有所说的性质. 于是

$$e_1 = e_1 e_2 = e_2.$$

这就证明了这种元素只有一个. $\square$

群 G 中具有性质 $ea = ae = a$(对所有的 $a \in G$) 的唯一的元素 e 称为群 G 的 **单位元素**. 显然，在通常乘法的情况下， 1 就是单位元素. 在通常加法情况下， 0 就是单位元素.

4. 对于群 G 中任一元素 a 有唯一元素 b 使 $ab = ba = e$.

证明 假设再有一个元素 c 也具有性质

$$ca = ac = e,$$

于是

$$c = ce = c(ab) = (ca)b = eb = b.$$

这就证明了唯一性. $\square$

对于元素 a, 唯一的具有性质

$$ab = ba = e$$

的元素 b 称为 a 的 **逆元素**, 记为 a^{-1}. 如果运算写成加法时， b 的逆元素记成 $-b$, 称为 b 的负元素.

由唯一性，不难看出， $(a^{-1})^{-1} = a$.

5. 对于群 G 中任意元素 a, b, 方程

$$ax = b$$

在 G 中有唯一解.

证明 显然，$x=a^{-1}b$ 是方程 $ax=b$ 的解，因而有解. 假设 x_1,x_2 是方程的两个解，于是有

$$ax_1=ax_2,$$

两边左乘 a^{-1}, 即得 $x_1=x_2$. 这就证明了解的唯一性. □

同样可证，在群 G 中方程 $ya=b$ 也有唯一解. 在上面的证明中可以看出，在群中，由 $ab=ac$ 可以推知 $b=c$.

群的定义中的结合律表明，群中三个元素 a,b,c 的乘积与作运算的顺序无关，因而可以简单地写成

$$abc$$

而不致产生混淆. 用数学归纳法，不难把这个结果推到任意多个元素，也就是说，在群 G 中，任意 l 个元素 $a_1,\cdots,a_l$ 的乘积与运算的顺序无关，因而可以简单地写成

$$a_1\cdots a_l.$$

据此，我们在群中可以定义元素的 **方幂**. 对于任意的正整数 n, 我们定义

$$a^n=a\cdot a\cdots a\ \ (n\text{个}),$$

即 n 个 a 连乘. 我们再约定

$$a^0=e,$$

$$a^{-n}=(a^{-1})^n,\ n\text{为正整数}.$$

于是 a^n 对任意整数 n 都有了意义，不难证明，对于任意整数 n,m, 任意元素 $a\in G$, 有

$$a^n\cdot a^m=a^{n+m},$$

$$(a^n)^m=a^{nm}.$$

这就是通常所谓的指数法则. 证明留给读者.

在群的定义中，我们没有要求群的运算适合交换律，即 $ab=ba$. 如果群 G 的运算适合交换律，那么群 G 就称为 **交换群** 或 **阿贝尔 (Abel) 群**. 例 1,2,3 中的群都是阿贝尔群，而例 4,5 中的群一般地不是阿贝尔群. 在阿贝尔群中，可以证明，对于任意元素 a,b, 任意整数 n, 有

$$(ab)^n=a^nb^n.$$

证明留给读者.

群 G 中元素的个数称为群 G 的 **阶**. 群 G 的阶记为 $|G|$. 如果 $|G|$ 是一有限数, 即 G 只含有有限多个元素, G 就称为 **有限群**. 如果 G 含有无限多个元素, G 就称为 **无限群**. 例 1,3,4,5 中的群是无限群, 而例 2 是有限群, 显然

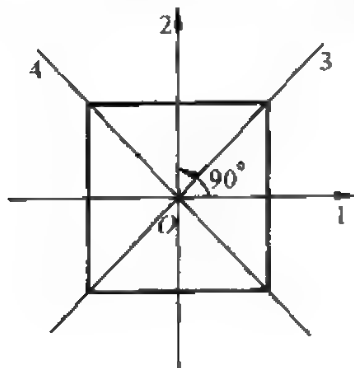
$$|U_n| = n.$$

§3 群的例子

在上一节我们已经看到许多特殊的群, 它们都是熟悉的. 现在再介绍两类重要的群.

1. 图形的对称群

设 F 是平面上的一个图形. 令 G_F 为全体保持 F 不变的 (从整体上说) 平面正交变换所成的集合. 显然, 恒等变换总在 G_F 中, 因而 G_F 是非空的; G_F 中任意两个变换的乘积仍在 G_F 中, 因而变换的乘法可以认为在 G_F 上定义的一个运算; G_F 中变换的逆也在 G_F 中. 这就是说, G_F 在变换的乘法下成一个群, 它称为 **图形 F 的对称群**.



例如 F 为一正方形 (如图), 显然, 保持这个正方形不变的正交变换只有: 绕 O 点转 $90°, 180°, 270°, 360°$ 以及对于直线 1,2,3,4 的镜面反射. 这 8 个正交变换就构成了正方形的对称群 G_F(证明留给读者). 如果我们用 T 表示绕 O 点转 $90°$, S 表示对于直线 1 的镜面反射, 那么不难看出, G_F 中 8 个元素就是

$$G_F = \{T, T^2, T^3, T^4, ST, ST^2, ST^3, ST^4\},$$

其中 $T^4 = I, S^2 = I, ST = T^{-1}S$.($I$ 表恒等映射)

类似地, 如果 F 是平面上正 n 边形, 那么 F 的对称群 G_F 是由 $2n$ 个元素组成. 令 T 为绕中心转 $\dfrac{2\pi}{n}$, S 为对于某一对称轴的镜面反射, 于是有

$$G_F = \{T, T^2, \cdots, T^n, ST, ST^2, \cdots, ST^n\},$$

其中 $T^n = I, S^2 = I, ST = T^{-1}S$. 这些群通常称为 **二面体群**, 用符号 D_n 表示.

2. 对称群 S_n

设 M 为一非空集合, 集合 M 到自身的可逆变换的全体对于变换的乘法显然组成一个群. 这个群称为 **集合 M 的全变换群**, 记为 $S(M)$. 当 M 为无限集合时, $S(M)$ 显然是一个无限群.

下面来看 M 是有限非空集合的情形. 当 M 含有 n 个元素时, M 的可逆变换称为 n 元 **置换**, $S(M)$ 称为 n **元对称群**, 简记为 S_n. 在 M 的元素用 $1,2,\cdots,n$ 编号之后, S_n 中元素 σ 可以表示为

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ \alpha_1 & \alpha_2 & \cdots & \alpha_n\end{pmatrix},$$

其中 $\alpha_i=\sigma(i), i=1,2,\cdots,n$.

因为 σ 是单射, 又是映上的, 所以下排 $\alpha_1\alpha_2\cdots\alpha_n$ 正好是 $1,2,\cdots,n$ 的一个排列. 这样就建立了 n 元置换与 n 阶排列之间的一个一一对应, 因之, $|S_n|=n!$. 按变换乘法的定义不难计算两个 n 元置换的乘积. 例如, 设

$$\sigma=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 1 & 3\end{pmatrix},\quad \tau=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 1 & 2 & 4\end{pmatrix}.$$

由

$$\sigma\tau(i)=\sigma(\tau(i)),\quad i=1,2,3,4.$$

于是

$$\sigma\tau=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 1 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 1 & 2 & 4\end{pmatrix}=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 4 & 3\end{pmatrix}.$$

如果一个 n 元置换 σ 将 $1,2,\cdots,n$ 中某 m 个数 $\alpha_1,\cdots,\alpha_m$ 轮换, 即

$$\sigma(\alpha_1)=\alpha_2,\ \sigma(\alpha_2)=\alpha_3,\cdots,$$
$$\sigma(\alpha_{m-1})=\alpha_m,\ \sigma(\alpha_m)=\alpha_1,$$

而保持其余的数不变, 那么 σ 称为一个 **轮换**. 我们简单地用

$$\sigma=(\alpha_1\alpha_2\cdots\alpha_m)$$

来表示这个轮换, 当 $m=2$ 时, σ 的作用是

$$\sigma(\alpha_1)=\alpha_2,\ \sigma(\alpha_2)=\alpha_1,$$

而保持其余的数不变, 这样的轮换称为 **对换**.

例如, 上面的 σ,τ 都是轮换, 即

$$\sigma=(1243),\quad \tau=(132),$$

而 $\sigma\tau$ 是一对换, 即

$$\sigma\tau=(34).$$

S_n 中两个轮换 $(\alpha_1\alpha_2\cdots\alpha_m)$ 与 $(\beta_1\beta_2\cdots\beta_l)$ 称为 **不相交的**, 如果

$$\alpha_i \neq \beta_j,\ i=1,2,\cdots,m, j=1,2,\cdots,l.$$

容易看出, 不相交的轮换对乘法是可以交换的. 下面来证明, 任何一个非单位的置换都能表成一些不相交的轮换的乘积, 而且表示法是唯一的.

设 σ 是一 n 元置换. 在 $1,2,\cdots,n$ 中任取一个元素 α_1, 用 σ 连续作用, 得一个序列

$$\alpha_2=\sigma(\alpha_1),\alpha_2=\sigma(\alpha_2),\cdots,$$

由于 $\alpha_i\in\{1,2,\cdots,n\},i=1,2,\cdots$, 所以序列中出现的元素必然有相同的. 令 α_j 为序列

$$\alpha_1,\alpha_2,\cdots$$

中第一个与它前面的某个元素, 比如说 α_i $(i<j)$, 相同的元素, 即 $\alpha_j=\alpha_i$, 或者

$$\sigma^{i-1}(\alpha_1)=\sigma^{j-1}(\alpha_1).$$

我们来证, $i=1$. 如 $i>1$, 用 σ^{-1} 作用上式的两边, 得

$$\sigma^{i-2}(\alpha_1)=\sigma^{j-2}(\alpha_1),$$

即

$$\alpha_{i-1}=\alpha_{j-1}.$$

这与 j 的选择矛盾, 因此必有 $i=1$, 即

$$\alpha_j=\alpha_1,$$

也就是

$$\sigma(\alpha_1)=\alpha_2,\cdots,\sigma(\alpha_{j-1})=\alpha_1,$$

σ 在元素 $\alpha_1,\alpha_2,\cdots,\alpha_{j-1}$ 上成一轮换, 我们再在 $\alpha_1,\cdots,\alpha_{j-1}$ 之外取一元素, 重复以上的讨论, 于是又得一个轮换, 因为 $\{1,2,\cdots,n\}$ 是一有限集合, 所以 σ 被分解成有限多个轮换的乘积,

$$\sigma=(\alpha_1\cdots\alpha_{j-1})\cdots$$

因为 σ 是一置换, 所以分解成的这些轮换必不相交, 证明留给读者, 唯一性显然.

下面是一个例子.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 4 & 6 \end{pmatrix} = (1\ 3\ 2)(4\ 5).$$

应该指出, $m=1$ 的轮换就是单位变换. 在置换的轮换表示中, 我们实际上是略去了所有一个数的轮换.

§4 子群、陪集

为了讨论群的问题, 子群是一个重要的概念.

定义 3 如果群 G 的非空子集合 H 对于 G 的运算也成一个群, 那么 H 称为 G 的 **子群**.

先来看几个例子.

例 1 设 n 为一正整数, 在整数加法群 $\mathbf{Z}$ 中所有 n 的倍数对加法显然成一群, 因而是 $\mathbf{Z}$ 的子群. 这个子群记为 $n\mathbf{Z}$.

例 2 设 V 是一欧氏空间. V 的正交变换群是 V 的可逆线性变换群的子群. 它们又都是 V(作为一个集合看) 的全变换群 $S(V)$ 的子群. 一般地, 对任意集合 M, $S(M)$ 的子群称为 **M 上的变换群**.

例 3 设 P 为一数域. 特殊线性群 $SL_n(P)$ 是一般线性群 $GL_n(P)$ 的子群.

例 4 设 $x_1, x_2, \cdots, x_n$ 是 n 个文字, 令

$$\begin{aligned} D(x_1, x_2, \cdots, x_n) = & \prod_{i<j}(x_i - x_j) \\ = & (x_1 - x_2)\cdots(x_1 - x_n) \\ & (x_2 - x_3)\cdots(x_2 - x_n)\cdots(x_{n-1} - x_n). \end{aligned}$$

对于 $\sigma \in S_n$, 我们定义

$$\begin{aligned} \sigma(D(x_1, x_2, \cdots, x_n)) = & D(x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(n)}) \\ = & \prod_{i<j}(x_{\sigma(i)} - x_{\sigma(j)}). \end{aligned}$$

显然有

$$\sigma(D(x_1, x_2, \cdots, x_n)) = \pm D(x_1, x_2, \cdots, x_n).$$

如果 $\sigma(D) = D$, σ 就称为 **偶置换**; 如果 $\sigma(D) = -D$, σ 就称为 **奇置换**. 不难看出, 全体偶置换组成 S_n 的一个子群. 这个群称为 n **元交错群**, 记为 A_n. 读者不难证明

$$|A_n| = \frac{1}{2}n!.$$

例 5 在群 G 中，仅由单位元素 e 组成的子集合 $\{e\}$ 显然是 G 的一个子群. 群 G 本身也是 G 的子群. 这两个子群称为 G 的 **平凡子群**, 其余的子群称为 **非平凡的**.

H 是 G 的子群可简记为 “$H < G$”.

群 G 的一个非空子集合 H 要适合什么条件才成为子群呢？

H 在包含元素 a,b 的同时必须包含 ab, 否则 G 的运算就不能被看作是 H 的运算. 子集合 H 的这个性质常常被说成是 H 对 G 的运算封闭. 其次， H 必须包含 G 的单位元素 e, H 在包含元素 a 的同时还必须包含 a 的逆元素 a^{-1}. 至于运算的结合律，在 H 中自然成立.

以上这些条件可以归结为：

定理 1 群 G 的非空子集合 H 是一子群的充分必要条件是：由 $a,b \in H$ 推出 $ab^{-1} \in H$.

证明 必要性是显然的. 我们来证充分性. 因 H 非空，所以 H 含有一个元素 a, 于是

$$aa^{-1} = e \in H.$$

由 $e,a \in H$ 即得 $ea^{-1} = a^{-1} \in H$. 由 $a,b \in H$ 可知 $b^{-1} \in H$, 从而

$$a(b^{-1})^{-1} = ab \in H.$$

这就证明了 H 是一个子群. □

显然，任意多个子群的交还是一子群. 证明留给读者.

设 H 是群 G 的一个子群. 对于 G 中任一元素 a, 我们称集合

$$\{ah \mid h \in H\}$$

为 H 的一个 **左陪集**, 简记为 aH. 因为 H 中有单位元素，所以 $a \in aH$. 同样，我们可以定义 **右陪集** 为

$$Ha = \{ha \mid h \in H\}.$$

显然， $h \mapsto ah$ 是子群 H 到左陪集 aH 的一个一一对应，同样， $h \mapsto ha$ 是子群 H 到右陪集 Ha 的一个一一对应. 因之，每个左 (右) 陪集与 H 有一样多的元素.

定理 2 设 H 是群 G 的一个子群. H 的任意两个左 (右) 陪集或者相等或者无公共元素. 群 G 可以表示成若干个不相交的左 (右) 陪集之并.

证明 设 aH, bH 是两个左陪集. 假如它们有公共元素，即有 $h_1, h_2 \in H$ 使

$$ah_1 = bh_2,$$

于是 $a = bh_2h_1^{-1} = bh_3$, 其中 $h_3 \in H$. 由

$$ah = bh_3h \in bH,$$

可知 $aH \subset bH$. 同样可证 $bH \subset aH$, 即

$$aH = bH.$$

这就证明了第一个论断.

因为 $a \in aH$, 所以

$$G = \bigcup_{a \in G} aH.$$

把其中重复出现的陪集去掉, 即得

$$G = \bigcup_{\alpha} a_\alpha H,$$

其中当 $\alpha \neq \beta$, 有 $a_\alpha H \cap a_\beta H = \emptyset$. 这就证明了第二点. 对右陪集完全一样地证明. □

推论 1 (**拉格朗日** (Lagrange) **定理**) *设 G 为一有限群, H 是一个子群. 于是 $|H|$ 是 $|G|$ 的因子.*

证明 设 $|G| = n, |H| = t$. 由定理 2, 有

$$G = a_1 H \cup \cdots \cup a_r H_r,$$

其中出现的陪集两两不相交. 因为 $|a_i H| = |H| = t$, 所以 $n = rt$. □

这是一个很重要的结论, 它给出了子群的一个重要的属性.

元素 a 称为左陪集 aH(右陪集 Ha) 的一个陪集代表. 从定理 2 的证明可以看出, 如果 $b \in aH$, 则 $bH = aH$. 这就表明, 陪集中任意一个元素都可以取作这陪集的代表.

在群 G 中, 任意一个元素 a 的全体方幂, 即集合

$$\{a^m, m \in Z\}$$

显然成一子群, 这个子群称为 **由 a 生成的子群**. 不难看出, 元素 a 的方幂或者两两全不同或者有一正整数 l 使 $a^l = e$. 事实上, 由

$$a^i = a^j,\ i < j,$$

即得

$$a^{j-i} = e.$$

在后一种情形，一定有一最小的正整数 d 使

$$a^d = e,$$

于是 $a, a^2, \cdots, a^d = e$ 就是 a 的全部不同的方幂，换句话说，a 生成的子群的阶为 d. 我们称元素 a 生成的子群的阶为**元素 a 的阶**. 由拉格朗日定理即得

推论 2 设 G 为一有限群. G 中每个元素的阶一定是 $|G|$ 的因子. 令 $|G| = n$, 对于 G 的每个元素 a 有

$$a^n = e.$$

证明 第一句话是显然的.

令元素 a 的阶为 d. 我们有 $n = dn_1$, 于是

$$a^n = a^{dn_1} = (a^d)^{n_1} = e^{n_1} = e. \quad \square$$

§5 群的同构

定义 4 设 G 与 G' 是两个群. 如果有一个 G 到 G' 的一一对应 σ, 它对于所有的 $x, y \in G$ 有

$$\sigma(xy) = \sigma(x)\sigma(y), \tag{1}$$

那么就称 G **同构于** G', 记作 $G \cong G'$. 适合 (1) 的一一对应称为 G 到 G' 的一个**同构映射**, 或简称**同构**.

由定义不难看出，同构映射把单位元素变到单位元素，把逆元素变到逆元素. 事实上，设 e 为 G 的单位元素，a 为 G 的任意一个元素，由 $ea = a$ 有 $\sigma(e)\sigma(a) = \sigma(a)$, 即 $\sigma(e)$ 为 G' 的单位元素 e'. 由 $a^{-1}a = e$ 有 $\sigma(a^{-1})\sigma(a) = e'$, 即 $\sigma(a^{-1}) = \sigma(a)^{-1}$.

下面来看几个例子.

例 1 我们知道，在 n 维线性空间中取一组基之后，全体可逆线性变换与全体 n 级可逆矩阵之间就建立了一个一一对应，并且这个对应具有性质 (1). 因之，数域 P 上 n 维线性空间中全体可逆线性变换组成的群与群 $GL_n(P)$ 同构. 基取得不同，我们就得到不同的同构映射. 由此可见，同构的群之间可以有不止一个同构映射.

如果群与群之间的映射具有性质 (1), 我们就说这个映射保持运算.

例 2 设 $\mathbf{R}$ 是全体实数对加法组成的群，$\mathbf{R}^+$ 是全体正实数对乘法组成的群. 显然，映射

$$\sigma(x) = \ln x$$

是 $\mathbf{R}^+$ 到 $\mathbf{R}$ 的一个一一对应，这里 ln 表示以 e 为底的自然对数. 我们知道

$$\sigma(xy) = \ln(xy) = \ln x + \ln y = \sigma(x) + \sigma(y).$$

因此，σ 是同构映射，它的逆映射为

$$\sigma^{-1}(x) = \mathrm{e}^x.$$

应该指出，正是这个同构的关系使我们能够利用对数来作实数的乘法.

容易看出，群的同构作为群之间的一种关系具有反身性，对称性与传递性，即它是一个等价关系：

1) $G \cong G$;

2) 由 $G \cong G'$ 推出 $G' \cong G$;

3) 由 $G \cong G'$ 与 $G' \cong G''$ 推出 $G \cong G''$.

因而群可以按同构加以分类. 证明留给读者.

定义表明，在同构映射下，对应的元素在各自的运算下有相同的代数性质. 在我们抽象地研究一个群时，同构的群是不必加以区别的.

从历史上看，群论最早是研究变换群的，而抽象群的概念正是从变换群抽象出来的. 下面的定理说明变换群在群中的重要地位.

定理 3 (凯莱 (Cayley) 定理) 任何一个群都同构于某一集合上的变换群.

证明 设 G 是一个群. 对于每个 $a \in G$，我们定义集合 G(注意，同一个 G!) 的变换 σ_a 如下：

$$\sigma_a(x) = ax,\ x \in G.$$

我们先证明，σ_a 是 G 的可逆变换. 显然，

$$\sigma_{a^{-1}}\sigma_a(x) = \sigma_{a^{-1}}(ax) = a^{-1}ax = x,$$

$$\sigma_a\sigma_{a^{-1}}(x) = \sigma_a(a^{-1}x) = aa^{-1}x = x.$$

这就是说，$\sigma_{a^{-1}}\sigma_a$ 与 $\sigma_a\sigma_{a^{-1}}$ 都是单位变换，即

$$\sigma_a^{-1} = \sigma_{a^{-1}},$$

因之，σ_a 是可逆变换. 这样，我们得到集合 G 的一些可逆变换组成的集合

$$G_l = \{\sigma_a \,|\, a \in G\}.$$

对于 $\sigma_a, \sigma_b \in G_l$，有

$$\sigma_a\sigma_b^{-1}(x) = \sigma_a\sigma_{b^{-1}}(x) = ab^{-1}x = \sigma_{ab^{-1}}(x),$$

即

$$\sigma_a\sigma_b^{-1}=\sigma_{ab^{-1}}\in G_l,$$

由定理 1, G_l 是一变换群.

因为

$$\sigma_a(e)=a,$$

所以当 $a\neq b$ 时, $\sigma_a\neq\sigma_b$. 这就说明, 映射

$$a\mapsto\sigma_a$$

是 G 到 G_l 的一个一一对应. 由

$$\sigma_a\sigma_b=\sigma_{ab}$$

可知上面的映射是一同构. 这就证明了定理.

变换 σ_a 称为由元素 a 在 G 上引起的 **左平移**, 而变换群 G_l 称为群 G 的 **左正则表示**.

如果我们定义 **右平移**

$$\tau_a(x)=xa^{-1},$$

那么同样可以证明, $G_r=\{\tau_a\,|\,a\in G\}$ 也是集合 G 的一个变换群, 也同构于 G. G_r 称为 G 的 **右正则表示**.

当 G 是有限群, $|G|=n$, G_l 与 G_r 都是 S_n 的子群. 作为定理 3 的特殊情形, 我们说, 任一有限群都同构于对称群的子群.

§6 同态、正规子群

为了研究群与群之间的关系, 同时也为了研究群的性质, 同态又是一个重要的概念.

定义 5 设 G 与 G' 是两个群, σ 是群 G 到 G' 的一个映射, 如果 σ 适合条件

$$\sigma(xy)=\sigma(x)\sigma(y),\ x,y\in G,$$

那么 σ 就称为 G 到 G' 的一个 **同态映射**, 或 **同态**.

显然, 同构都是同态. 与同构的情形一样, 可以证明 $\sigma(e)=e',\sigma(a^{-1})=\sigma(a)^{-1}$, 其中 e 与 e' 分别为群 G 与 G' 的单位元素.

下面看几个例子.

例 1 设 G 与 G' 是两个群，e' 是 G' 的单位元素．定义 $\sigma(x)=e'$，对所有的 $x\in G$，这当然是一同态．但这个同态并没有给出 G 与 G' 之间有任何实质性的关系．

例 2 对于任意 $A\in GL_n(P)$，定义

$$\sigma(A)=|A|,$$

也就是行列式．令 P^* 是数域 P 中非零元素对于乘法组成的群，由 $|AB|=|A||B|$ 可知 σ 是 $GL_n(P)$ 到 P^* 的一个同态．

例 3 令

$$D(x_1,\cdots,x_n)=\prod_{i<j}(x_i-x_j),$$

我们知道，对于 $\sigma\in S_n$ 有

$$\begin{aligned}\sigma D(x_1,\cdots,x_n)=&\ D(x_{\sigma(1)},\cdots,x_{\sigma(n)})\\=&\ \prod_{i<j}(x_{\sigma(i)}-x_{\sigma(j)})=\pm D(x_1,\cdots,x_n).\end{aligned}$$

定义

$$\sigma D(x_1,\cdots,x_n)=\mathrm{sgn}(\sigma)D(x_1,\cdots,x_n),$$

sgn 就是由 S_n 到乘法群 $\{1,-1\}$ 的一个映射．显然 sgn 是一同态．

当 σ 为 G 到 G' 的一个同态，我们常常简记为

$$\sigma:G\to G'.$$

如果 $\sigma:G\to G'$，定义

$$\sigma G=\{\sigma(a)\,|\,a\in G\}.$$

显然 σG 是 G' 的一个子群，它称为同态 σ 的**象**．

在同态定义中，对于映射 σ 我们既不要求它是映上的，也不要求它是单射．如果 $\sigma:G\to G'$ 是映上的，即 $\sigma G=G'$，我们就称 σ 为**满同态**．如果 $\sigma:G\to G'$ 是单射，即 G 与 σG 同构，也就是 G 与 G' 的一个子群同构，我们就称 σ 为**单一同态**，或者**嵌入映射**．

对于同态 $\sigma:G\to G'$，对于任一 $a'\in G'$，我们考虑集合

$$\{x\in G\,|\,\sigma(x)=a'\},$$

这个集合可能是空集合 (当 $a' \notin \sigma G$), 也可能包含一个以上的元素. 我们称这个集合为元素 a' 的 **完全反象**, 记为 $\sigma^{-1}(a')$. 特别地, 单位元素的完全反象 $\sigma^{-1}(e')$ 称为同态 σ 的 **核**. 同态 σ 的核记为 $\ker(\sigma)$.

我们来证明, 同态的核是群 G 的子群. 由 $\sigma(e) = e'$ 可知 $e \in \ker(\sigma)$; 如果 $a, b \in \ker(\sigma)$, 即 $\sigma(a) = \sigma(b) = e'$, 则 $\sigma(ab^{-1}) = \sigma(a)\sigma(b)^{-1} = e'$, 因之 $\ker(\sigma)$ 是 G 的一个子群.

设 $\ker(\sigma) = H$, 而 aH 为一个左陪集. 如果 $x \in aH$, 即 $x = ah$, 则 $\sigma(x) = \sigma(ah) = \sigma(a)\sigma(h) = \sigma(a)$. 这就表明, 陪集 aH 中元素全有相同的象. 反过来, 如果 $\sigma(x) = \sigma(a)$, 那么 $\sigma(x) \cdot \sigma(a)^{-1} = e', \sigma(xa^{-1}) = e'$, 即

$$xa^{-1} \in H, \ x \in aH.$$

这就说明, 所有以 $\sigma(a)$ 为象的元素全在陪集 aH 中. 综上所述, 我们得到, 如果 $\sigma(a) = a'$, 那么

$$\sigma^{-1}(a') = aH.$$

我们知道, 群 G 分解成子群 H 的不相交的左陪集之并, 同态 σ 给出了这些左陪集与 σG 的元素之间的一个一一对应.

完全一样地可以证明, 当 $\sigma(a) = a'$ 时,

$$\sigma^{-1}(a') = Ha.$$

因之同态的核还具有性质

$$aH = Ha, \ 对所有的\ a \in G.$$

定义 6 设 H 是群 G 的子群. 如果对于所有的元素 $a \in G$ 有 $aH = Ha$, 那么 H 称为 **正规子群**.

上面的讨论说明, 同态的核都是正规子群.

正规子群的定义可以改写为

$$aHa^{-1} = H, \ 对所有的\ a \in G.$$

正规子群的定义换个说法就是子群 H 的左右陪集相等.

显然, 在交换群中, 每个子群都正规.

在上面的例 2 中, 对于 $A \in GL_n(P)$,

$$\sigma(A) = |A|.$$

显然，$\ker(\sigma) = SL_n(P)$，因而 $SL_n(P)$ 是 $GL_n(P)$ 的一个正规子群. 直接由行列式的性质也不难验证 $SL_n(P)$ 是正规子群.

在例 3 中，由 A_n 的定义可知，同态 sgn 的核就是 A_n. 因而 A_n 是 S_n 的正规子群.

因为整数加法群 $\mathbf{Z}$ 是交换群，所以它的子群 $n\mathbf{Z}$ 是正规子群.

在 S_3 中，$A_3 = \{e, (123), (132)\}$ 是正规子群，但子群 $H = \{e, (12)\}$ 就不正规.

当 H 是 G 的正规子群时，我们记为 $H \lhd G$.

§7 商群

在群中我们定义子集合的运算.

设 A, B 是群 G 的两个子集合，定义

$$AB = \{ab \mid a \in A, b \in B\},$$

即由 A 中元素与 B 中元素相乘所得的集合. 子集乘积满足结合律：$(AB)C = A(BC)$.

如 A 为一子群，$B = \{b\}$，即由单个元素 b 所成的集合，那么 AB 就是子群 A 的一个右陪集.

对于任一子集合 A，我们定义

$$A^{-1} = \{a^{-1} \mid a \in A\},$$

即由 A 中元素的逆元素组成的集合.

利用集合运算，定理 1 可以改写成：群 G 中非空子集合 H 是一子群的充分必要条件为

$$HH^{-1} \subset H.$$

如果 H 是任意一个子群，那么两个右陪集 Ha, Hb 的积 $(Ha)\cdot(Hb)$ 不一定还是右陪集. 但是对于正规子群，我们有如下的重要事实.

定理 4 *设 H 是群 G 的一个子群. H 是正规子群的充分必要条件为任意两个左 (右) 陪集之积还是一左 (右) 陪集.*

证明 先证必要性. 设 H 是一正规子群，Ha, Hb 是两个右陪集，于是

$$(Ha)(Hb) = H(aH)b = H(Ha)b = Hab.$$

再证充分性. 设 Ha, Hb 是任意两个右陪集. 由条件 $(Ha)\cdot(Hb) = Hc$. 显然 $ab \in (Ha)(Hb)$, 即 $ab \in Hc$, 因之

$$(Ha)(Hb) = Hc = Hab.$$

两边用 b^{-1} 右乘, 得

$$HaH = Ha.$$

因为 $e \in H$, 所以 $aH \subset HaH$, 即

$$aH \subset Ha,$$

或者

$$aHa^{-1} \subset H, \text{ 对所有的 } a \in G.$$

把 a 换成 a^{-1}, 就有

$$a^{-1}Ha \subset H, \text{ 即 } H \subset aHa^{-1},$$

从而

$$aHa^{-1} = H, \text{ 对所有的 } a \in G.$$

这就证明了 H 是正规子群. □

令 G/H 代表正规子群 H 的全部不同的右陪集组成的集合.

定理 4 说明, 在集合 G/H 上可以定义一个乘法, 即

$$(Ha)(Hb) = Hab.$$

在这个乘法下, 它是否成一个群呢?

由 $(Ha)(Hb) = Hab$ 可以看出, 陪集之间的乘法实际上就归结为陪集代表的乘法. 因之, 结合律是显然的. 由

$$H \cdot Ha = Ha = Ha \cdot H$$

可知, H 是单位元素. 再由

$$(Ha^{-1})(Ha) = H$$

可知, 每个元素有逆元素. 这说明了, G/H 在陪集的运算下确实成一群.

定义 7 G/H 在陪集的乘法下所成的群称为 G 对正规子群 H 的 **商群**. 仍记为 G/H.

因为对于正规子群, 左陪集也就是右陪集, 所以 G/H 也可以看成是左陪集所组成的群.

下面来看一个重要的例子. 设 $n>1$ 是一正整数, 我们知道, $n\mathbf{Z}$ 是 $\mathbf{Z}$ 的一个正规子群. 在 $\mathbf{Z}$ 中运算是加法, 因而陪集就写成

$$n\mathbf{Z}+r=\{nk+r\mid k\in\mathbf{Z}\}.$$

我们知道, 每个整数 x 都可以唯一地表成

$$x=qn+r,\quad 其中\ 0\le r<n,$$

r 称为余数. 不难看出, 两个整数属于同一个陪集的充分必要条件为它们有相同的余数. 由此可知, $\mathbf{Z}$ 对于 $n\mathbf{Z}$ 的全部陪集为

$$n\mathbf{Z}, n\mathbf{Z}+1,\cdots,n\mathbf{Z}+(n-1).$$

如果用 $\overline{0},\overline{1},\cdots,\overline{(n-1)}$ 代表这 n 个陪集, 那么它们之间的运算就是

$$\bar{i}+\bar{j}=\begin{cases}\overline{i+j}, & 当\ i+j<n,\\ \overline{i+j-n}, & 当\ i+j\ge n.\end{cases}$$

如果 G 是有限群, 那么显然有

$$|G/H|=\frac{|G|}{|H|}.$$

设 $H\lhd G$, 我们定义

$$\varphi(a)=Ha,$$

显然,

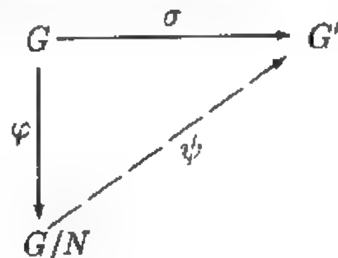
$$\varphi(ab)=Hab=HaHb=\varphi(a)\varphi(b).$$

因之, φ 是 G 到 G/H 的一个同态, 映上是明显的. 这个同态称为群 G 到它的商群的 **自然同态**. 自然同态的核就是正规子群 H. 这就说明, 不但同态的核是正规子群, 而且每个正规子群也都是某一同态的核.

下面的定理进一步弄清楚同态与正规子群的关系.

定理 5 (**群同态基本定理**) 设 $\sigma:G\to G'$ 是一满同态, N 为 σ 的核. 于是 G/N 与 G' 同构.

证明 设 $\varphi:G\to G/N$ 是自然同态. 我们有两个满同态 σ 和 φ, 如下图:



图中虚线则表示我们要找的一个同构. 定义

$$\psi(Na)=\sigma(a),$$

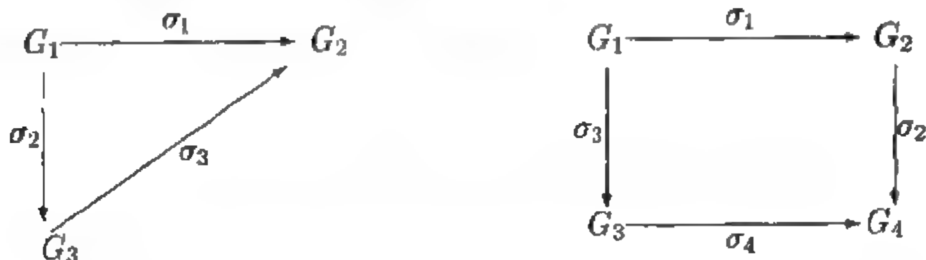
因为 σ 是一满同态，即 $\sigma(G)=G'$, 所以前面的分析表明 ψ 是 G/N 到 G' 的一个一一对应. 容易验证,

$$\begin{aligned}\psi(NaNb) &= \psi(Nab)=\sigma(ab)\\ &= \sigma(a)\sigma(b)=\psi(Na)\psi(Nb),\end{aligned}$$

这就是说， $\psi: G/N\to G'$ 是一同构，因而 G/N 与 G' 同构. □

从 ψ 的定义立即看出， $\psi\varphi=\sigma$.

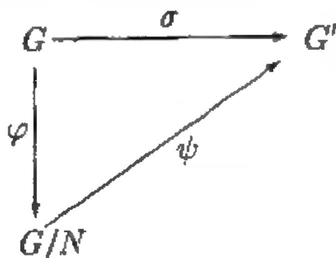
在我们考察几个群之间的一些同态时，常常用点来代表群，它们之间的同态用箭头来表示，这样就得到一个有向图. 如



其中 G_i 代表群， σ_i 代表同态. 在这两个图中，如果我们分别有

$$\sigma_3\sigma_2=\sigma_1 \text{ 与 } \sigma_2\sigma_1=\sigma_4\sigma_3,$$

那么我们就说这些图是 **交换的**. 用这样的术语，定理与证明中得到的结果可以说成：存在一同构 $\psi: G/N\to G'$ 使图形交换.



为了研究一个群的性质，我们常常需要找到这个群的一些同态象. 定理 5 告诉我们，找同态象的问题可以归结为找这个群的正规子群的问题.

我们知道, $\sigma(A)=|A|$ 是 $GL_n(P)$ 到 P^* 的一个满同态, 而 $\ker(\sigma)=SL_n(P)$. 由定理 5 即得

$$GL_n(P)/SL_n(P)\cong P^*.$$

§8 环、子环

群是具有一个代数运算的代数结构. 下面来介绍具有两个代数运算的代数结构.

定义 8 设 L 是一非空集合, 在 L 上定义了两个代数运算, 一个叫加法, 记为 $a+b$, 一个叫乘法, 记为 ab. 如果具有性质:

1) L 对于加法成一个交换群;

2) 乘法的结合律: 对所有的 $a,b,c\in L$,

$$a(bc)=(ab)c;$$

3) 乘法对加法的分配律: 对所有的 $a,b,c\in L$,

$$a(b+c)=ab+ac,$$
$$(b+c)a=ba+ca;$$

那么 L 就称为一个 **环**.

下面来看几个例子.

例 1 全体整数对通常的加法与乘法成一环, 称为 **整数环**, 记为 $\mathbf{Z}$. 所有的数域都是环.

例 2 全体偶数对通常的加法与乘法也成一环. 一般地, 取整数 $m>1$, 整数中全体 m 的倍数 $m\mathbf{Z}$ 对通常的加法与乘法也是环.

例 3 设 P 为一数域, 全体系数在 P 中的 n 级矩阵对矩阵的加法与乘法成一环, 这个环记为 $M_n(P)$. 全体整系数的 n 级矩阵也成一环 $M_n(\mathbf{Z})$. 一般地, 设 L 为一环, 全体系数取自 L 的 n 级矩阵对矩阵的加法与矩阵乘法也成一环 $M_n(L)$.

例 4 在全体整数的集合上, 取通常的加法, 但把乘法定义为 $ab=0$, 对所有的 $a,b\in\mathbf{Z}$, 我们也得到一个环. 由单个的零所成的集合 $\{0\}$, 对通常的加法与乘法也成一环.

由定义可以推出环的一些基本性质.

1. 用 0 代表环中加法群的零元素, 于是对所有的 $a\in L$ 有 $a0=0a=0$.

证明 取 $b\in L$, 有

$$ab=a(b+0)=ab+a0,$$

即得 $a0=0$. 同样可证 $0a=0$. □

2. 对所有的 $a,b\in L$, 有

$$(-a)b=a(-b)=-ab,$$
$$(-a)(-b)=ab.$$

证明 由

$$(-a)b+ab=(-a+a)b=0b=0,$$

即得

$$(-a)b=-ab.$$

同样可证 $a(-b)=-ab$.

$$(-a)(-b)=-a(-b)=-(-ab)=ab.$$

3. 因为 L 对加法成一交换群，所以对于正整数 n, 我们可以定义

$$na=a+\cdots+a\ (n个).$$

我们还可以定义

$$0a=0\ (左边是整数\ 0),$$

$$(-n)a=n(-a).$$

于是对任意整数 n,m, 任意 $a,b\in L$, 有

$$(n+m)a=na+ma,$$
$$n(ma)=(nm)a,$$
$$n(a+b)=na+nb.$$

同样，对正整数 n, 可以定义

$$a^n=a\cdots a\ (n个).$$

对于正整数 n,m 有

$$a^na^m=a^{n+m},$$
$$(a^n)^m=a^{nm}.$$

在环中，一般地不能定义 a^0 与 a^{-n}.

定义 9 设 S 是环 L 的一个非空子集合. 如果 S 对于 L 的两个运算也成一环，那么 S 称为 L 的一个 **子环**.

容易看出，子集合 S 是子环的充分必要条件为：S 对于加法是一子群并且对于乘法是封闭的.

我们来看几个例子.

例 1 整数环 $\mathbf{Z}$ 是有理数域 $\mathbf{Q}$ 的子环. 设 $n>1$, $n\mathbf{Z}$ 是 $\mathbf{Z}$ 的子环.

例 2 设 P 是一数域. 在 $M_n(P)$ 中，全体对角矩阵组成一子环；全体数量矩阵也组成一子环；全体上 (下) 三角矩阵组成一子环.

例 3 设 R 为实数域. 令 C' 为 $M_2(R)$ 中全体形状为

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \quad a,b \in \mathbf{R}$$

的矩阵所成的集合. 这种形式的矩阵对加法成一子群是明显的, 由计算

$$\begin{aligned} &\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} \\ = &\begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}, \end{aligned}$$

可见 C' 对乘法封闭. 因之, C' 是 $M_2(\mathbf{R})$ 的一个子环.

例 4 设 $\mathbf{C}$ 为复数域. 令 H 为 $M_2(\mathbf{C})$ 中全体形状为

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}, \quad \alpha,\beta \in \mathbf{C}$$

的矩阵所成的集合. 这种形式的矩阵对加法成一子群是明显的, 由计算

$$\begin{aligned} &\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}\begin{pmatrix} \gamma & \delta \\ -\overline{\delta} & \overline{\gamma} \end{pmatrix} \\ = &\begin{pmatrix} \alpha\gamma-\beta\overline{\delta} & \alpha\delta+\beta\overline{\gamma} \\ -\overline{\alpha}\overline{\delta}-\overline{\beta}\gamma & \overline{\alpha}\overline{\gamma}-\overline{\beta}\delta \end{pmatrix} \\ = &\begin{pmatrix} \alpha\gamma-\beta\overline{\delta} & \alpha\delta+\beta\overline{\gamma} \\ -\overline{(\alpha\delta+\beta\overline{\gamma})} & \overline{(\alpha\gamma-\beta\overline{\delta})} \end{pmatrix}, \end{aligned}$$

可知 H 对乘法封闭. 因之, H 是 $M_2(\mathbf{C})$ 的一个子环.

例 5 在 $M_3(P)$ 中全体形式为

$$\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad a,b,c,d \in P$$

的矩阵显然构成一个子环.

与群一样, 环也有同构的概念.

定义 10 设 L 与 L' 是两个环, 如果有一个 L 到 L' 的一一对应 σ, 它具有性质:

1) $\sigma(a+b)=\sigma(a)+\sigma(b)$;

2) $\sigma(ab)=\sigma(a)\sigma(b)$,

其中 $a,b\in L$; 那么 L 就称为与 L' 同构. 具有以上性质的映射 σ 称为一个 **同构映射**(或简称 **同构**).

因为环的同构映射自然是它们加法群之间的同构映射, 所以群同构的性质这里当然也有, 不必重新推导了.

显然, 环的同构也具有反身性、对称性与传递性.

环的同构的例子是很多的. 例如, 设 V 是数域 P 上的一个 n 维线性空间, V 的全体线性变换所成的集合 $L(V)$ 对线性变换的加法与乘法显然组成一个环. 在 V 中取定一组基之后, 我们就建立了 $L(V)$ 到 $M_n(P)$ 的一个一一对应. 因为这个对应保持加法与乘法, 所以它是一同构映射. 这就是说, 环 $L(V)$ 与环 $M_n(P)$ 同构. 取不同的基, 我们就有不同的同构映射. 由此可见, 同构的环之间可以有不止一个同构映射.

设 $\mathbf{C}$ 为复数域. 我们定义

$$\sigma(a+bi)=\begin{pmatrix} a & b \\ -b & a \end{pmatrix},\quad a,b\in\mathbf{R}.$$

不难看出, σ 是 $\mathbf{C}$ 到 C'(上面例 3) 的一个一一对应, 而且保持运算 (读者验证一下). 因之, σ 是 $\mathbf{C}$ 到 C' 的一个同构映射. 也就是说, 例 3 中的 C' 与复数域 $\mathbf{C}$ 同构.

上面例 5 中的子环明显地与 $M_2(P)$ 同构.

§9 各种特殊类型的环

从环的定义可以看出, 整数环 $\mathbf{Z}$ 与矩阵环 $M_n(P)$ 是环的重要原型. 但环的定义所要求的比这两个具体的环的性质要少, 而在以后的研究中我们碰到的环常常具有一些其它性质. 现在就来介绍环的一些重要类型.

设 L 是一环. 如果 L 中有一元素 e 具有性质:

$$ea=ae=a,\quad \text{对所有的 } a\in L,$$

那么 e 称为环 L 的 **单位元素**. 容易证明, 如果环 L 有单位元素, 那只能有一个. 具有单位元素的环简称 **幺环**, 幺环的单位元素简记为 1. 明显地, 环 $\mathbf{Z}$ 与 $M_n(P)$ 都是幺环, 而全体偶数 $2\mathbf{Z}$ 所成的环就不是幺环.

如果幺环 L 的一对元素 a,b 满足 $ab=1$, 则 $b(a)$ 称为 $a(b)$ 的右 (左) 逆. 如果 a 既有右逆又有左逆, 则 a 的左、右逆相等, 它简称为 a 的逆. 此时 a 称为

L 的一个可逆元素，也叫做 L 的一个 **单位**. 显然幺环 L 的全部单位构成的集合对乘法成一群，称为 L 的 **单位群**.

设 $a \in L, a \neq 0$. 如果有元素 $b \in L, b \neq 0$ 使 $ab = 0$, 那么元素 a 就称为一个 **左零因子**. 同样可以定义 **右零因子**. 我们知道，环 $M_n(P), n \geq 2$, 有零因子，而环 $\mathbf{Z}$ 就没有零因子.

如果环 L 没有零因子，那么在环 L 中 **消去律** 成立，即由 $ab = ac, a \neq 0$ 可以推出 $b = c$. 事实上，由 $ab = ac$ 得

$$ab - ac = 0 \text{ 即 } a(b - c) = 0.$$

因为 $a \neq 0$, 且 L 无零因子，所以

$$b - c = 0 \text{ 即 } b = c.$$

如果环 L 的乘法适合交换律，即

$$ab = ba,\ a, b \in L,$$

那么 L 称为 **交换环**. 整数环 $\mathbf{Z}$ 是交换环，而环 $M_n(P)$ $(n > 1)$ 就不是.

定义 11 无零因子的交换幺环，且 $1 \neq 0$, 就称为 **整环**.

条件 $1 \neq 0$ 就等价于环中至少含有两个元素．(证一下!)

显然整数环 $\mathbf{Z}$ 是整环.

定义 12 如果环 F 是交换幺环，至少含两个元素，且全体非零元素对乘法成一群，那么环 F 称为 **域**.

域 F 的全体非零元素对乘法成一个交换群就意味着，F 中每个非零元素 a 都有逆元素 a^{-1}, 即 $a^{-1}a = 1$.

既然每个非零元素 a 都有逆元素 a^{-1}, 因之由 $ab = 0, a \neq 0$ 可知 $b = a^{-1}(ab) = 0$. 这就是说，域中没有零因子. 从而域一定是整环. 显然整数环 $\mathbf{Z}$ 不是域，这就表明，整环不一定是域.

定理 6 有限整环是域.

证明 设 L 为一含有 n 个元素的整环，它的元素为

$$a_1, a_2, \cdots, a_n, \text{ 其中 } a_1 = 1.$$

取 L 中任一非零元素 a, 作元素

$$aa_1, aa_2, \cdots, aa_n.$$

由消去律可以知道，这 n 个元素必两两不同．即当 $i \neq j$ 时，有 $aa_i \neq aa_j$．因之它们就是 L 的全部元素，其中必有 1．换句话说，必有 a_k 使 $aa_k = 1$．这就证明了，L 中每个非零元素都有逆元素，因而 L 是域． □

如果域 F 的一个子环 S 是一个域，则称 S 是 F 的一个 **子域**．

显然，所有的数域都是域．每个数域都包含有理数域作为它的子域，因而都是无限域．至于像定理 6 中所说的有限域，在 §11 中我们再给出具体的例子．

在域的定义中，如果不要求乘法的交换性，我们就有体的概念．

定义 13 如果环 L 是幺环，至少含有两个元素，且全体非零元素对乘法成一个群，那么 L 称为 **体**．

显然，所有的域都是体．下面来看一个乘法不交换的体的例子．

在上一节子环的例 4 中，H 表示全体形式为

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}, \quad \alpha, \beta \in \mathbf{C}$$

的矩阵所成的环．取 $\alpha = 1, \beta = 0$，即得单位矩阵，因而 H 是一幺环．由

$$\begin{vmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{vmatrix} = \alpha\overline{\alpha} + \beta\overline{\beta} = |\alpha|^2 + |\beta|^2$$

可知，只要 α, β 不全为零，即

$$X = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \neq 0,$$

X 就可逆，而

$$X^{-1} = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}^{-1} = \frac{1}{|\alpha|^2 + |\beta|^2} \begin{pmatrix} \overline{\alpha} & -\beta \\ \overline{\beta} & \alpha \end{pmatrix}$$

仍属于 H．这就是说，H 的全体非零元素对乘法成一个群，从而 H 是体．

令 $\alpha = a + bi, \beta = c - di$，于是 H 中元素为

$$\begin{aligned} \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} &= \begin{pmatrix} a - bi & c + di \\ -c + di & a - bi \end{pmatrix} \\ &= a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix} \\ &\quad + c \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + d \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}. \end{aligned}$$

用 I, J, K 分别代表矩阵

$$\begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix},$$

单位矩阵就写成 1, 那么 H 的元素就可以表示成

$$a + bI + cJ + dK,$$

其中 a, b, c, d 为实数. 直接计算矩阵即得

$$I^2 = J^2 = K^2 = -1,$$
$$IJ = K = -JI, JK = I = -KJ,$$
$$KI = J = -IK.$$

由此可见, H 不适合乘法的交换律.

H 通常称为 **四元数体**.

§10 环的同态、理想

环也有同态的概念, 在代数中这是一个重要的概念.

定义 14 设 L, L' 是两个环, σ 是 L 到 L' 的一个映射. 如果对于所有的 $a, b \in L$, σ 具有性质:

1) $\sigma(a+b) = \sigma(a) + \sigma(b)$;

2) $\sigma(ab) = \sigma(a)\sigma(b)$;

那么 σ 就称为环 L 到 L' 的一个 **同态映射**(或简称 **同态**), 有时简记为 $\sigma : L \to L'$.

环的同态当然是 L 的加法群到 L' 的加法群的同态, 因之

$$\sigma(0) = 0, \quad \sigma(-a) = -\sigma(a).$$

由同态的定义立即看出, $\sigma(L)$ 是 L' 的一个子环. 如果 $\sigma(L) = \{0\}$, 则 σ 称为 **零同态**; 如果 $\sigma(L) = L'$, 则我们说 σ 是一个 **满同态**, 而 L' 就称为 L 的一个 **同态象**.

显然, 同构是同态的特殊情形.

下面来看几个例子.

例 1 设 L 是一个环, 考虑集合 L^n, 即以 L 中元素为分量的全体 n 元有序

组所成的集合．在 L^n 上按分量定义加法与乘法，即定义

$$\begin{aligned}(a_1,\cdots,a_n)+(b_1,\cdots,b_n)\\=(a_1+b_1,\cdots,a_n+b_n),\\(a_1,\cdots,a_n)(b_1,\cdots,b_n)\\=(a_1b_1,\cdots,a_nb_n).\end{aligned}$$

不难看出，L^n 在这样定义的运算下成一环．

我们定义

$$\sigma((a_1,\cdots,a_n))=a_1,$$

显然 σ 是环 L^n 到环 L 的一个满同态．

例 2 在 $M_4(\mathbf{Q})$ 中全体形状为

$$\begin{pmatrix}A & B\\ 0 & C\end{pmatrix}.$$

其中 $A,B,C\in M_2(\mathbf{Q})$, 的矩阵显然成一子环，记这个子环为 L. 定义

$$\sigma\left(\begin{pmatrix}A & B\\ 0 & C\end{pmatrix}\right)=A,$$

σ 是环 L 到环 $M_2(\mathbf{Q})$ 的一个同态．这个同态也是满的．

例 3 定义在实数域上的全体连续函数，在函数的加法与乘法下成一环．这个环通常记为 $C[-\infty,+\infty]$. 设 a 是一个取定的实数．定义

$$\sigma(f(x))=f(a),\ f(x)\in C[-\infty,+\infty].$$

σ 是环 $C[-\infty,+\infty]$ 到实数域 $\mathbf{R}$ 的一个同态．

对于环的同态同样有核的概念．设 $\sigma:L\to L'$. 我们定义 σ 的核为

$$\ker(\sigma)=\{a\in L\,|\,\sigma(a)=0\}.$$

我们知道，环的同态也是它们的加法群之间的同态．这里定义的核与作为加法群的同态的核是一致的，因之，$\ker(\sigma)$ 是 L 的加法群的一个子群，而且 σ 是单射当且仅当 $\ker(\sigma)=\{0\}$.

如果 $a,b\in\ker(\sigma)$, 那么

$$\sigma(ab)=\sigma(a)\sigma(b)=0,$$

即 $ab \in \ker(\sigma)$. 这就是说，同态 σ 的核是 L 的一个子环. 由上面的证明可以看出，为了使 $\sigma(ab)=0$ 只要求 a,b 之一属于 σ 的核就行了. 换句话说，如果 $a \in \ker(\sigma)$, r 为 L 中任意元素，那么

$$\sigma(ra) = \sigma(r)\sigma(a) = \sigma(r)0 = 0,$$
$$\sigma(ar) = \sigma(a)\sigma(r) = 0\sigma(r) = 0,$$

即 $ra, ar \in \ker(\sigma)$.

由此可见，同态的核不仅是子环，而且是一种特殊类型的子环. 对于这种子环，我们引入

定义 15 设 L 是一环， $I \subset L$ 是 L 的一个加法子群. 如果对于任意 $r \in L, a \in I$ 都有

$$ra \in I.\ ar \in I,$$

那么 I 称为 L 的一个 **理想**(或称 **双边理想**). 如果 L 的一个加法子群 I 只满足 $ra \in I$(或 $ar \in I$) 对于任意 $r \in L, a \in I$, 则 I 称为 L 的一 **左**(或 **右**)**理想**.

在整数环 $\mathbf{Z}$ 中，子环 $m\mathbf{Z}$ $(m > 0)$ 是一个理想.

在环 $C[-\infty,+\infty]$ 中，不难证明对于固定的实数 a, 集合

$$\{f(x) \in C[-\infty,+\infty] \mid f(a) = 0\}$$

是一个理想. 这个理想正是上面例 3 中定义的同态的核.

显然， $\{0\}$ 与 L 都是环 L 的理想，它们称为 **平凡的理想**. 当 L 是一个幺环，任何一个非平凡的理想都不可能含有单位元素. （为什么？）

§11 商环

我们看到，同态的核是一个理想. 是不是每个理想都是某一同态的核呢？首先，对于环 L 中一个给定的理想 I, 我们仿照商群的构造法来定义商环，然后对上面的问题给出肯定的回答.

设 I 是环 L 的一个理想. I 作为 L 的加法群的子群， L 的元素按 I 分成陪集

$$r + I,\ \ r \in L.$$

因为加法群是交换的，所以陪集之间可以定义加法，即

$$(r_1 + I) + (r_2 + I) = r_1 + r_2 + I.$$

现在来证明，任意两个陪集之积仍属于某一陪集，设

$$x = r_1 + a \in r_1 + I, \text{ 其中 } a \in I,$$
$$y = r_2 + b \in r_2 + I, \text{ 其中 } b \in I.$$

于是

$$\begin{aligned} xy = & (r_1 + a)(r_2 + b) \\ = & r_1 r_2 + a r_2 + r_1 b + ab \in r_1 r_2 + I, \end{aligned}$$

即

$$(r_1 + I)(r_2 + I) \subset r_1 r_2 + I.$$

我们定义

$$(r_1 + I)(r_2 + I) = r_1 r_2 + I.$$

由上面的证明可以看出，两个陪集的乘积与所乘的陪集代表 r_1, r_2 无关，因而这个定义是合理的.

由于陪集的运算实际上都归结为陪集代表的运算，也就是 L 中元素的运算，所以不难验证乘法的结合律与分配律. 因之，全体陪集所成的集合在这样规定的运算下成一环.

定义 16 设 I 是环 L 的一个理想. L 对于 I 的陪集在上面定义的运算下所成的环称为 L 对于 I 的 **商环**, 记为 L/I.

容易看出，映射

$$\sigma(a) = a + I,\ a \in I$$

是环 L 到商环 L/I 的一个满同态，这个同态的核就是理想 I. 这就肯定地回答了上面提出的问题，即每个理想都是某个同态的核.

作商环是一个重要的构造环的方法, 下面来看一个例子, 设 n 为一正整数, 我们知道, $n\mathbf{Z}$ 是整数环 $\mathbf{Z}$ 中的一个理想. 商环 $\mathbf{Z}/n\mathbf{Z}$ 是由下列陪集

$$n\mathbf{Z}, n\mathbf{Z} + 1, \cdots, n\mathbf{Z} + (n-1)$$

组成. 前面已经分析过它们之间的加法，至于乘法，按商环的运算的定义,

$$(n\mathbf{Z} + i)(n\mathbf{Z} + j) = n\mathbf{Z} + ij = n\mathbf{Z} + r,$$

其中 r 为 ij 被 n 除所得的余数，即

$$ij = nq + r, \text{ 其中 } 0 \le r < n.$$

如果这 n 个陪集仍用

$$\overline{0}, \overline{1}, \cdots, \overline{n-1}$$

表示，那么就有

$$\bar{i}\cdot\bar{j}=\bar{r},$$

其中

$$ij=nq+r,\quad 0\le r<n.$$

这样，对于任意正整数 n，我们就作出了一个含有 n 个元素的环．我们称 $\mathbf{Z}/n\mathbf{Z}$ 为 **整数模 n 的环**．

现在考察环 $\mathbf{Z}/n\mathbf{Z}$ 的单位群．若 $\bar{i}$ 是一个可逆元，则存在元素 $\bar{j}$ 使得 $\bar{i}\cdot\bar{j}=\bar{1}$．这意味着 $i\cdot j\equiv 1\pmod n$．从而 $(i,n)=1$．反之，若 $(i,n)=1$，则存在整数 j,k 使得 $i\cdot j+kn=1$．从而有 $\bar{i}\cdot\bar{j}=\bar{1}$．所以环 $\mathbf{Z}/n\mathbf{Z}$ 的单位群由全部与 n 互素的陪集 $i+n\mathbf{Z}$，$(i,n)=1$，所组成．这个群记作 $(\mathbf{Z}/n\mathbf{Z})^*$．它的阶等于欧拉函数 $\varphi(n)$(参看第零章 §5)．一个重要的情况是，当 n 为素数时，$\varphi(n)=n-1$．这表明，$\mathbf{Z}/n\mathbf{Z}$ 的单位群由全部非 0 元素组成．因而 $\mathbf{Z}/n\mathbf{Z}$ 是一个域．这就给出了一批有限域．它们是与数域很不一样的域．在下一节我们要讨论它们的差异．

最后我们指出，与定理 5 相仿，我们有

定理 7 *如果 $\sigma: L\to L'$ 是一满同态，I 为 σ 的核，那么商环 L/I 与 L' 同构．*

证明留给读者．

§12 特征

域是一种很重要的代数结构，在数学中经常要碰到．在这一节我们要介绍域的一个重要的数量属性．

设 F 是一个域．我们来考虑域 F 的单位元素 e 在 F 的加法群中的阶．如果 e 是一有限阶元素，即存在一最小的正整数 m 使

$$me=0.$$

显然 $m>1$．我们来证明，m 必为素数．用反证法，假如 m 不是素数，我们有 $m=m_1m_2$，其中 $1<m_1<m, 1<m_2<m$，于是

$$me=(m_1e)(m_2e)=0.$$

由 $m_1e\neq 0, m_2e\neq 0$，而域中无零因子，上式不可能成立．这就证明了，如果域中单位元素 e 是有限阶元素，它的阶必是素数．

定义 17 设 F 是一域．如果 F 的单位元素 e 在 F 的加法群中是有限阶元素，阶为 p，那么就称域 F 的 **特征为 p**，如果单位元素是无限阶元素，那么就称域 F 的 **特征为 0**．域的特征通常记为 $\chi(F)$．

由上面的讨论可知，$\chi(F)$ 或者是 0 或者是一素数 p, 显然，数域的特征全为 0. 而有限域 $\mathbf{Z}/p\mathbf{Z}$ 的特征为 p.

设 a 为域 F 中任一非零元素. 由

$$ma = mae = a(me)$$

可知，$ma = 0$, 当且仅当 $me = 0$. 因之在域的加法群中，任一非零元素都与单位元素有相同的阶. 这就说明，域的特征也就是域的非零元素在加法群中共同的阶.

设 $\chi(F) = 0$, b 为域 F 的任一元素，n 为正整数. 我们来看方程

$$nx = b.$$

由 $nx = (ne)x$, $ne \neq 0$ 可知 $(ne)^{-1}b$ 是方程 $nx = b$ 的唯一解. 这个解通常就简写成

$$\frac{1}{n}b.$$

应该看到，对 $\chi(F) \neq 0$ 的域，$\frac{1}{n}b$ 就不一定都有意义.

最后我们证明

定理 8 设 F 为一域. 如果 $\chi(F) = 0$, 那么 F 包含一子域与有理数域 $\mathbf{Q}$ 同构. 如果 $\chi(F) = p \neq 0$, 那么 F 包含一子域与 $\mathbf{Z}/p\mathbf{Z}$ 同构.

证明 定义整数环 $\mathbf{Z}$ 到 F 的映射 σ 为

$$\sigma(n) = ne.$$

容易验证，σ 是一同态映射. 如果 $\chi(F) = p \neq 0$, 那么 $\ker(\sigma) = p\mathbf{Z}$, 而 σ 的象为

$$\mathbf{F}_p = \{e, \cdots, (p-1)e, 0\}.$$

由定理 7,$\mathbf{F}_p$ 与 $\mathbf{Z}/p\mathbf{Z}$ 同构.

如果 $\chi(F) = 0$, 那么 σ 是单射. σ 的象

$$R_0 = \{ne,\ n \in \mathbf{Z}\}$$

与整数环同构. 因为当 $n \neq 0$ 时，$ne \neq 0$, 所以 σ 可以扩充到有理数域 $\mathbf{Q}$, 即定义

$$\sigma\left(\frac{m}{n}\right) = (ne)^{-1}(me).$$

容易证明，当

$$\frac{m}{n} = \frac{m'}{n'},$$

就有

$$\sigma\left(\frac{m}{n}\right)=\sigma\left(\frac{m'}{n'}\right).$$

因之上面的定义是合理的. σ 的象

$$F_0=\{(ne)^{-1}(me),\ n,m\in\mathbf{Z},n\neq 0\}$$

显然是 F 的一个子域，它与有理数域 $\mathbf{Q}$ 同构. 这就完成了证明. □

定理 8 表明，任意一个域必然包含域 $\mathbf{Q}$, $\mathbf{Z}/p\mathbf{Z}$ 中的一个作为子域，其中 p 为素数 (在同构的意义下). 因之，可以认为有理数域 $\mathbf{Q}$ 与整数模 p 的域 $\mathbf{Z}/p\mathbf{Z}$ 是一些最小的域. 它们统称为 **素域**.

习 题

1. 如果在群 G 中，对于任意元素 a,b 有 $(ab)^2=a^2b^2$, 则 G 为交换群.

2. 如果在群 G 中，每个元素 a 都适合 $a^2=e$, 则 G 为交换群.

3. 设 G 是一非空的有限集合，其中定义了一个乘法 ab, 适合条件:

(i) $a(bc)=(ab)c$;

(ii) $ab=ac\Rightarrow b=c$;

(iii) $ac=bc\Rightarrow a=b$;

证明 G 在这个乘法下成一群.

4. 设 G 是一非空集合并在 G 内定义了一个乘法 $a\cdot b$. 证明，如果乘法满足结合律，并且对于任一对元素 $a,b\in G$, 下列方程

$$ax=b \text{ 和 } ya=b$$

分别在 G 内恒有解，则 G 在这乘法下成一群.

5. 在 S_3 中找出两个元素 x,y, 适合

$$(xy)^2\neq x^2y^2.$$

6. 对于 $n>2$, 作一阶为 $2n$ 的非交换群.

7. 设 G 是一群，$a,b\in G$, 如果 $a^{-1}ba=b^r$, 其中 r 为一正整数. 证明 $a^{-i}ba^i=b^{r^i}$.

8. 证明：群 G 为一交换群当且仅当映射 $x\mapsto x^{-1}$ 是一同构映射.

9. 设 S 为群 G 的一个非空子集合，在 G 中定义一个关系 $a\sim b$ 当且仅当 $ab^{-1}\in S$. 证明这是一等价关系的充分必要条件为 S 是一子群.

10. 设 n 为一正整数，$n\mathbf{Z}$ 为整数加法群 $\mathbf{Z}$ 的一个子群，证明 $n\mathbf{Z}$ 与 $\mathbf{Z}$ 同构.

11. 证明：在 S_4 中，子集合

$$B=\{e,(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$$

是一子群. 证明群 B 与 U_4 不同构.

12. 证明: 如果在一阶为 $2n$ 的群中有一 n 阶子群, 它一定是正规子群.

13. 设群 G 的阶为一偶数, 证明 G 中必有一元素 $a \neq e$ 适合 $a^2 = e$.

14. 令

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} e^{\frac{2\pi i}{n}} & 0 \\ 0 & e^{-\frac{2\pi i}{n}} \end{pmatrix},$$

证明集合 $\{B, B^2, \cdots, B^n, AB, AB^2, \cdots, AB^n\}$ 在矩阵的乘法下成一群, 而这个群与群 D_n 同构.

15. 设 i 为一正整数. 如果群 G 中任意元素 a, b 都适合 $(ab)^k = a^k b^k$, $k = i, i+1, i+2$, 证明 G 为交换群.

16. 在群 $SL_2(\mathbf{Q})$ 中, 证明元素

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

的阶为 4, 元素

$$b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

的阶为 3, 而 ab 为无限阶元素.

17. 如果 G 为一交换群, 证明 G 中全体有限阶元素组成一子群.

18. 如果群 G 只有有限多个子群, 证明 G 为有限群.

19. 写出群 D_n 的全部正规子群.

20. 设 H, K 为群 G 的子群, 证明 HK 为一子群当且仅当 $HK = KH$.

21. 设 H, K 为有限群 G 的子群. 证明

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

22. 设 M, N 是群 G 的正规子群. 证明:

(i) $MN = NM$;

(ii) MN 是 G 的一正规子群;

(iii) 如果 $M \cap N = \{e\}$, 那么 MN/N 与 M 同构.

23. 设 G 是一个群, S 是 G 的一非空子集合. 令

$$C(S) = \{x \in G \mid xa = ax, \text{ 对一切 } a \in S\},$$
$$N(S) = \{x \in G \mid x^{-1}Sx = S\}.$$

证明:

(i) $C(S), N(S)$ 都是 G 的子群;

(ii) $C(S)$ 是 $N(S)$ 的正规子群.

24. 证明任意一个 2 阶群都与乘法群 $\{1, -1\}$ 同构.

25. 试定出所有互不同构的 4 阶群.

26. 设 p 为一素数. 证明任意两个 p 阶群必同构.

27. $\mathbf{Z}$ 为整数环, 在集合 $S=\mathbf{Z}\times\mathbf{Z}$ 上定义

$$(a,b)+(c,d)=(a+c,b+d),$$
$$(a,b)\cdot(c,d)=(ac+bd,ad+bc).$$

证明 S 在这两个运算下成一具有单位元素的环.

28. 在整数集 $\mathbf{Z}$ 上重新定义加法 "$\oplus$" 与乘法 "$\odot$" 为

$$a\oplus b=ab,\qquad a\odot b=a+b.$$

试问 $\mathbf{Z}$ 在这两个运算下是否成一环.

29. 设 L 为一具有单位元素的交换环, 在 L 中定义:

$$a\oplus b=a+b-1,$$
$$a\odot b=a+b-ab.$$

证明在新定义的运算下, L 仍成一具有单位元素的交换环, 并且与原来的环同构.

30. 给出环 L 与它的一个子环 S 的例子, 它们分别具有下列性质:

1) L 具有单位元素, 单 S 无单位元素;

2) L 没有单位元素, 但 S 有单位元素;

3) L、S 都有单位元素, 但不相同;

4) L 不交换, 但 S 交换.

31. 环 L 中元素 e_L 称为一个左单位, 如果对所有的 $a\in L$,

$$e_La=a;$$

元素 e_R 称为一个右单位, 如果对所有的 $a\in L$,

$$ae_R=a.$$

证明:

(i) 如果 L 既有左单位又有右单位, 则 L 具有单位元素.

(ii) 如果 L 有左单位, L 无零因子, 则 L 具有单位元素.

(iii) 如果 L 有左单位, 但没有右单位, 则 L 至少有两个左单位.

32. 设 F 为一域. 证明 F 无非平凡的双边理想.

33. 如果 L 是一交换环, $a\in L$.

(i) 证明 $La=\{ra\mid r\in L\}$ 是一双边理想;

(ii) 举例说明, 如果 L 非交换, 则 La 不一定是双边理想.

34. 设 I 是交换环 L 的一个理想, 令

$$\operatorname{rad} I=\{r\in L\mid r^n\in I \text{ 对某一正整数 } n\},$$

证明 $\text{rad}\, I$ 也是一理想. $\text{rad}\, I$ 叫做理想 I 的**根**.

35. 设 L 为一具有单位元素的交换环. 如果 L 没有非平凡的理想, 则 L 是一域.

36. $\mathbf{Q}$ 为有理数域, $M_n(\mathbf{Q})$ 为 n 阶有理系数全矩阵环. 证明 $M_n(\mathbf{Q})$ 无非平凡的理想 (这种环称为**单环**)

37. 设 L 为一环, a 为 L 中一非零元素. 如果有一非零元素 b 使 $aba = 0$. 证明 a 是一左零因子或一右零因子.

38. 环中元素 x 称为一**幂零元素**, 如果有一正整数 n 使 $x^n = 0$. 设 a 为具有单位元素的环中一幂零元素, 证明 $1 - a$ 可逆.

39. 证明: 在交换环中, 全体幂零元素的集合是一理想.

40. 设 L 为一具有单位元素的有限环. 证明由 $xy = 1$ 可得 $yx = 1$.

41. 在一具有单位元素的环中, 如果对元素 a 有 b 使 $ab = 1$ 但 $ba \neq 1$, 则有无穷多个元素 x, 适合 $ax = 1$.

42. 设 L 是一个至少有两个元素的环. 如果对于每个非零元素 $a \in L$ 都有唯一的元素 b 使得

$$aba = a.$$

证明:

(i) L 无零因子;

(ii) $bab = b$;

(iii) L 有单位元素;

(iv) L 是一个体.

43. 令 $C[0,1]$ 为全体定义在闭区间 $[0,1]$ 上的连续函数组成的环. 证明:

(i) 对于 $C[0,1]$ 的任一非平凡的理想 I, 一定有一实数 θ, $0 \leq \theta \leq 1$, 使 $f(\theta) = 0$ 对所有的 $f(x) \in I$;

(ii) $f(x) \in C[0,1]$ 是一零因子当且仅当点集

$$\{x \in [0,1] \mid f(x) = 0\}$$

包含一个开区间.

44. 令 $F = \mathbf{Z}/p\mathbf{Z}$ 为 p 个元素的域. 求

(i) 环 $M_n(F)$ 的元素的个数;

(ii) 群 $GL_n(F)$ 的元素的个数.

45. 设 K 是一体, $a, b \in K$, a, b 不等于 0, 且 $ab \neq 1$. 证明**华罗庚恒等式**:

$$a - (a^{-1} + (b^{-1} - a)^{-1})^{-1} = aba.$$

(提示: 先证对任意 $x \neq 0, 1$, 有 $(x^{-1} - 1)^{-1} = (1 - x)^{-1} - 1$.)

第二章　群

在我们知道了群的定义及群的一些最基本的性质之后，我们现在来介绍群论中几个常用的结果，同时也引入一些必要的概念．本章讨论的问题没有紧密的逻辑联系，但通过这些问题的讨论，读者可以初步接触到群论的方法．

§1　群的同态定理

设 N 是群 G 的一个正规子群，作商群 G/N，令

$$\pi : G \to G/N$$

是群到商群的自然同态．我们首先指出，在同态 π 下，商群 G/N 的全部子群与群 G 中所有包含 N 的子群之间有一个一一对应．由商群的定义，对于 G 中任何一个包含 N 的子群 $H, \pi(H)$ 显然是 G/N 中一个子群．另一方面，对于 G/N 中的子群 $\overline{H}$，我们定义

$$\pi^{-1}(\overline{H}) = \{x \in G \mid \pi(x) \in \overline{H}\}.$$

因为 $\overline{H}$ 中的单位元素就是陪集 N，所以容易看出，$\pi^{-1}(\overline{H})$ 不但是 G 的一个子群，而且一定包含 N．由于 π 是满同态，所以

$$\pi(\pi^{-1}(\overline{H})) = \overline{H}.$$

由 π^{-1} 的定义可知，对于 G 的任意子群 H，有

$$\pi^{-1}(\pi(H)) \supset H.$$

我们来证明，当 $H \supset N$ 时，

$$\pi^{-1}(\pi(H)) = H.$$

设 $x \in \pi^{-1}(\pi(H))$，即 $\pi(x) \in \pi(H)$，因而有 $h \in H$ 使 $\pi(x) = \pi(h)$．由 π 的定义即得

$$x \in hN \subset H,$$

这就证明了 $\pi^{-1}(\pi(H)) = H$．以上讨论表明，同态 π 建立了 G 中所有包含 N 的子群与 G/N 中全部子群之间的一个一一对应．

如果 H 是 G 的一个包含 N 的正规子群，即对于所有的 $x \in G$，有

$$x^{-1}Hx = H,$$

那么

$$\pi(x^{-1}Hx) = \pi(x)^{-1}(\overline{H})\pi(x).$$

由 π 是满同态可知，$\pi(H)$ 在 G/N 中也正规. 反过来，如果 $\overline{H}$ 是 G/N 的一个正规子群，那么对于所有的 $x \in G$,

$$\pi(x^{-1}\pi^{-1}(\overline{H})x) = \pi(x)^{-1}\overline{H}\pi(x) = \overline{H},$$

即

$$x^{-1}\pi^{-1}(\overline{H})x \subset \pi^{-1}(\overline{H}).$$

这就是说，$\pi^{-1}(\overline{H})$ 也是 G 的正规子群. 因之，同态 π 也建立了 G/N 中全部正规子群与 G 中所有包含 N 的正规子群之间的一一对应.

对于 G/N 中正规子群 $\overline{H}$ 作商群

$$(G/N)/\overline{H}.$$

令

$$\varphi: G/N \to (G/N)/\overline{H}$$

为自然同态. 于是 $\varphi\pi$ 是群 G 到 $(G/N)/\overline{H}$ 的同态. 因为 φ 的核是 $\overline{H}$, 所以 $\varphi\pi$ 的核就是 $\pi^{-1}(\overline{H}) = H$. 由同态基本定理，我们有

$$G/H \cong (G/N)/\overline{H}.$$

由 $\pi^{-1}(\overline{H}) = H$ 可知，$\pi(H) = \overline{H}$ 且 $H \supset N$. $\overline{H}$ 作为 G/N 的子群可以与 H/N 等同起来，因而以上的同构可以写成

$$G/H \cong (G/N)/(H/N).$$

综上所述，我们有

定理 1 *设 N 为群 G 的一个正规子群，而 $\pi: G \to G/N$ 为自然同态. π 建立了 G 中所有包含 N 的子群与 G/N 中全部子群之间一个一一对应. 在这个对应下，正规子群与正规子群相对应. 如果 $H \lhd G, H \supset N$, 那么*

$$G/H \cong (G/N)/(H/N). \quad \square$$

如果 $\sigma: G \to G'$ 是一满同态，而 σ 的核为正规子群 K, 那么由同态基本定理我们有同构

$$G/K \cong G'.$$

利用这个同构，定理 1 可以改写成较为一般的形式.

定理 2 设 $\sigma: G \to G'$ 为一满同态，而 $\ker(\sigma) = K$，于是 σ 给出了 G 中所有包含 K 的子群与 G' 中全部子群之间的一个一一对应，即对于 $H < G, H \supset K$，

$$H \mapsto \sigma(H) = H' < G'.$$

在这个对应下，$H \lhd G$ 当且仅当 $H' \lhd G'$. 如果 $H \lhd G, H \supset K, \sigma(H) = H'$，那么有

$$G/H \cong G'/H'. \quad \square$$

下面来考虑同态映射对于任意一个子群的作用. 设 $N \lhd G, \pi: G \to G/N$，而 H 是 G 的任意一个子群. 显然，$\pi(H)$ 是 G/N 中一个子群. 限制在 H 上，π 的核为 $H \cap N$，而 $H \cap N$ 显然是 H 的一个正规子群，由同态基本定理，我们有

$$H/H \cap N \cong \pi(H).$$

另一方面，我们不难验证 HN 是 G 的一个子群. 任取 $h_1, h_2 \in H, n_1, n_2 \in N$，

$$(h_1n_1)(h_2n_2) = h_1h_2(h_2^{-1}n_1h_2)n_2 \in HN,$$
$$(h_1n_1)^{-1} = n_1^{-1}h_1^{-1} = h_1^{-1}(h_1n_1^{-1}h_1^{-1}) \in HN.$$

这就证明了，$HN < G$. 显然有 $N \subset HN$，且

$$\pi(HN) = \pi(H).$$

由同态基本定理，我们有

$$HN/N \cong \pi(H).$$

综合上面两个同构，我们得到

定理 3 设 $H < G, N \lhd G$. 于是我们有同构

$$HN/N \cong H/H \cap N. \quad \square$$

按以上的讨论，定理中的同构就是：对于任意 $x \in H$，

$$xN \to x(H \cap N).$$

定理 1(或 2) 与定理 3，连同以前的同态基本定理，习惯上统称为群的**同态定理**.

对于任意的同态 $\sigma: G \to G'$, 如果 G 为阿贝尔群, 那么同态象 $\sigma(G)$ 一定也是阿贝尔群. 反过来, 如果象 $\sigma(G)$ 是阿贝尔群, 那么 G 不一定是阿贝尔群, 在这个情况下, 我们要问, σ 的核具有什么特点呢?

为了说清楚这个问题, 我们引入一个以后常用的名词. 设 G 是一个群, S 是 G 的一个非空子集合. 考虑 G 中所有包含 S 的子群. 我们知道, 任意多个子群的交还是子群, 因之, 所有包含 S 的子群的交还是一个包含 S 的子群, 显然, 它包含在每一个包含 S 的子群之中, 在这个意义上, 它是最小的一个包含 S 的子群. 我们称这个子群为 **由 S 生成的子群**, 记为 $\langle S\rangle$, 也就是

$$\langle S\rangle = \bigcap_{S\subset H<G} H.$$

既然 $\langle S\rangle$ 包含 S, 也就包含 S^{-1}, 从而 $\langle S\rangle$ 就一定包含集合 $S\cup S^{-1}$ 中任意有限多个元素的乘积, 即

$$x_1x_2\cdots x_m, \qquad \text{其中 } x_1,\cdots,x_m \in S\cup S^{-1}.$$

不难验证, 所有可以表成上述形式的元素组成的集合是 G 的一个子群, 这个子群包含 S 且包含在 $\langle S\rangle$ 中. 由 $\langle S\rangle$ 的定义可知, 这个子群就是 $\langle S\rangle$.

如果 $\langle S\rangle = G$, 那么 S 就称为 G 的一组 **生成元**. 如果在群 G 中存在一有限集合 S 使

$$\langle S\rangle = G,$$

那么群 G 就称为 **有限生成的**. 显然, 有限群一定是有限生成的, 反过来当然不一定. 由一个元素生成的群称为 **循环群**.

设 $\sigma: G\to G'$ 为一满同态, 且 G' 交换. 对于任意的 $a,b\in G$, 有

$$\sigma(a^{-1}b^{-1}ab) = \sigma(a)^{-1}\sigma(b)^{-1}\sigma(a)\sigma(b) = e,$$

即 $a^{-1}b^{-1}ab\in \ker(\sigma)$. 元素 $a^{-1}b^{-1}ab$ 称为群 G 元素 a,b 的 **换位子**, 简记为 $[a,b]$. 由所有换位子生成的子群称为 G 的 **换位子群**, 记为 $G^{(1)}$, 上面的讨论表明, 对于同态

$$\sigma: G\to G',$$

如果 $\sigma(G)$ 交换, 那么 $G^{(1)}\subset \ker(\sigma)$. 读者不难证明, 如果 $G^{(1)}\subset\ker(\sigma)$, 则 $\sigma(G)$ 一定交换, 而且 $G^{(1)}$ 为 G 的正规子群.

§2 循环群

由一个元素生成的群称为循环群. 根据上节的讨论, 如果 a 是循环群 G 的一个生成元, 那么群 G 的元素都可以表示成 a 的方幂, 因而循环群是交换群.

循环群可以认为是最简单的一类群. 我们现在来讨论循环群的结构, 循环群的子群以及判断一个群是不是循环群的条件. 整数加法群 $\mathbf{Z}$ 是循环群, 1 是 $\mathbf{Z}$ 的一个生成元. 在群 $\mathbf{Z}$ 中, 取任一整数 m, m 的全体倍数构成一个子群 $m\mathbf{Z}$. $m\mathbf{Z}$ 是由 m 生成的群. 实际上, 这样的子群就是 $\mathbf{Z}$ 的全体子群.

定理 4 整数加群 $\mathbf{Z}$ 的子群都是由某一非负整数 m 生成的循环群. 对于 $m, n \geq 0, n\mathbf{Z} \supset m\mathbf{Z}$ 当且仅当 $n|m$, 即 n 是 m 的因子.

证明 设 H 是 $\mathbf{Z}$ 的一个子群. 如果 H 不是由单个的 0 组成的群, 那么 H 中含有非零数, 因而 H 中含有正数. 在 H 所含的正数中, 令 m 为最小数, 我们来证明, $H = m\mathbf{Z}$. 设 x 为 H 的任一元素, 由整数的除法算式, 有

$$x = qm + r, \text{ 其中 } q, r \in \mathbf{Z}, \ 0 \leq r < m.$$

$r = x - qm \in H$, 如 $r \neq 0$, 则 r 是 H 中一个比 m 更小的正数, 这与 m 的选择不符. 因而 $r = 0$, 即 $x = qm$. 既然 m 在 H 中, m 的倍数当然也在 H 中, 这就证明了 $H = m\mathbf{Z}$.

当 $H = \{0\}$ 时, 就取 $m = 0$.

由 $n\mathbf{Z} \supset m\mathbf{Z}$ 可知 $m \in n\mathbf{Z}$, 即 $n|m$.

由 $n|m$ 可知, m 的倍数都是 n 的倍数, 即 $n\mathbf{Z} \supset m\mathbf{Z}$. □

弄清楚了整数加群的子群的情况之后, 我们现在来讨论一般的循环群. 设 G 为一循环群, g 是 G 的一个生成元, 即 $G = \langle g \rangle$. 定义由整数加群 $\mathbf{Z}$ 到群 G 的同态 φ 为:

$$\varphi(n) = g^n, \ \ n \in \mathbf{Z}.$$

显然 φ 是一满同态. 考察 φ 的核 $N = \ker(\varphi)$. 如果 $N = \{0\}$, 那么 φ 为一同构, $\varphi : \mathbf{Z} \cong G$. 这时 G 称为**无限循环群**. 既然无限循环群与 $\mathbf{Z}$ 同构, 无限循环群的可能的子群也就清楚了. 如果 $N \neq \{0\}$. 由定理 4, $N = m\mathbf{Z}$, 其中 m 是一正整数, 于是由同态基本定理,

$$G \cong \mathbf{Z}/m\mathbf{Z},$$

m 就是元素 g 的阶, $G = \{g, \cdots, g^{m-1}, g^m = e\}$. 由定理 2, G 的子群与 $\mathbf{Z}$ 中包含 $m\mathbf{Z}$ 的子群成一一对应, 根据定理 4, 这些子群就是

$$s\mathbf{Z}, \qquad \text{其中 } s|m, s > 0,$$

它们在 G 中的象就是 $\langle g^s \rangle$, 阶为 $\dfrac{m}{s}$.

总结以上讨论, 我们有

定理 5 无限循环群都与 $\mathbf{Z}$ 同构, 它的子群正如定理 4 所描述的, 与全体非负整数成一一对应. 阶为 m 的循环群 $G=\langle g\rangle$ 同构于 $\mathbf{Z}/m\mathbf{Z}$, 对于 m 的每个正因子 s 都存在唯一的一个 s 阶子群, 这个子群为

$$\langle g^{\frac{m}{s}}\rangle. \quad \square$$

利用循环群的结果, 我们顺便讨论一下群中元素的阶.

推论 设群 G 的元素 g 的阶为正整数 m. 于是 $g^l=e$ 当且仅当 $m|l$. 对于任意正整数 s, 元素 g^s 的阶为 $\dfrac{m}{(m,s)}$, 这里 (m,s) 为 m 与 s 的最大公因子.

证明 定义同态 $\varphi:\mathbf{Z}\to\langle g\rangle$ 为

$$\varphi(n)=g^n,$$

我们知道 $\ker(\varphi)=m\mathbf{Z}$, 这就说明 $g^l=e$ 当且仅当 $l\in m\mathbf{Z}$, 即 $m|l$.

$\langle g^s\rangle$ 是 m 阶循环群 $\langle g\rangle$ 的一个子群. 我们知道, 循环群 $\langle g\rangle$ 的子群具有形式 $\langle g^d\rangle$. 其中 $d|m$, 由 $\langle g^s\rangle=\langle g^d\rangle$ 得

$$s=nd+vm,$$
$$d=ts+wm.$$

由第一式可知 $d|s$, 再由第二式可知

$$d=(m,s).$$

$\langle g^d\rangle$ 的阶为 $\dfrac{m}{d}$, 因而 g^s 的阶为 $\dfrac{m}{d}$. $\square$

下面我们要给出一有限交换群是循环群的判别条件, 为此, 我们先给出有限交换群的一个性质.

引理 设交换群 G 中元素 g,h 的阶分别为 m,n, 且 $(m,n)=1$. 于是元素 gh 的阶为 mn.

证明 设 gh 的阶为 l. 由

$$(gh)^l=e$$

有 $(gh)^{lm}=e$, 即 $h^{lm}=e$. 根据上面的推论, 有 $n|lm$. 由 $(n,m)=1$ 即得

$$n|l.$$

同理可证 $m|l$. 由 $(m,n)=1$ 有 $mn|l$.

另一方面, $(gh)^{mn}=g^{mn}h^{mn}=e$, 于是 $l|mn$. 因之, $l=mn$. $\square$

定理 6 设 G 为一有限交换群. 于是在 G 中存在一个元素, 它的阶是 G 中所有元素的阶的倍数.

证明 取 G 中一个具有最大阶的元素 g, 它的阶为 n. 我们来证明, G 中所有元素的阶都是 n 的因子, 用反证法, 假如有一个元素 g_1, 它的阶 n_1 不是 n 的因子, 由 $n_1 \nmid n$ 可知, 存在一素数的方幂 p^r, 使

$$p^r | n_1, \text{ 但 } p^r \nmid n.$$

令

$$n_1 = p^r \cdot l, \quad n = p^s \cdot m,$$

其中

$$s < r, \quad (m, p) = 1.$$

于是元素 g_1^l 与 g^{p^s} 的阶分别为 p^r 与 m, 由引理, 元素 $g_1^l g^{p^s}$ 的阶为

$$p^r m > p^s m = n.$$

这与 n 的选择矛盾. □

由定理 6 即得循环群的判别条件.

定理 7 设 G 为一有限交换群. G 为循环群的充分必要条件是对于所有正整数 m, 在 G 中适合方程 $x^m = e$ 的元素个数不超过 m.

证明 先证充分性.

按定理 6, 在 G 中有一个元素 g, 它的阶 n 是 G 中所有元素的阶的倍数. 换句话说, 群 G 中所有元素都适合方程

$$x^n = e.$$

由定理的条件, $|G| \leq n$. 显然, $n \leq |G|$, 因而 $|G| = n$. 这就证明, $G = (g)$ 为循环群.

由循环群的性质, 不难证明必要性, 证明留给读者. □

§3 单群与 A_n 的单性

定义 1 如果群 G 没有非平凡的正规子群, 那么群 G 称为 **单群**.

交换单群的情况是清楚的.

定理 8 设 G 为交换群, $G \neq \{e\}$, G 为单群的充分必要条件是 G 为素数阶的循环群.

证明 因为在交换群中，所有的子群都正规，所以在交换单群中没有非平凡的子群.

在 G 中任取一非单位的元素 g, 既然 G 没有非平凡的子群，就有 $G=\langle g\rangle$, 即 G 为循环群. 由定理 5, 没有非平凡子群的循环群只能是素数阶的循环群. 同样根据定理 5, 素数阶的循环群没有非平凡的子群. □

非交换的单群的情况要复杂得多. 在某种意义上说，单群是构成各种群的基础. 设 G 有一非平凡的正规子群 N, 作商群 G/N, 我们很自然地可以问，正规子群 N 与商群 G/N 的结构在多大程度上能够决定群 G 的结构. 群扩张理论就是研究这个问题的. 根据群扩张理论，群 G 的结构可由正规子群 N 与商群 G/N 作原则的刻画. 因之，相当长的时期中，决定有限单群的结构一直是有限群的研究中一个重要的课题. 近二十年来，这方面的发展很迅速，目前问题已经解决，也就是说，我们已经可以给出全部的有限单群. 这是代数学在 20 世纪的一个重大成就.

在这里我们当然无法讨论这样一个大问题，下面我们只是给出一类有限非交换的单群，换句话说，我们要证明， A_n, $n\geq 5$, 是非交换单群.

为了这个目的，我们对于置换还需要作些讨论.

引理 *每个置换都可以表示成一些对换的乘积；每个偶置换都可以表示成一些长度为 3 的轮换 (简称 3- 轮换) 的乘积.*

证明 我们知道，每个置换都可以表示成一些轮换的乘积. 对于每个轮换，直接验证可知

$$(i_1 i_2 \cdots i_r)=(i_1 i_r)\cdots(i_1 i_2),$$

因而每个置换都可以表示成一些对换的乘积.

容易看出， $\operatorname{sgn}(i,j)=-1$, 即对换都是奇置换. 因之，当偶置换分解成对换的乘积时，其中出现的对换的个数一定是偶数. 为了证明第二个论断，我们只需要证明任意两个不同的对换的乘积一定能表示成 3- 轮换的乘积就行了. 设 i,j,k,l 为四个不同的数，我们有

$$\begin{aligned}(ij)(ik)&=(ikj),\\(ij)(kl)&=(ij)(jk)(jk)(kl)\\&=(jki)(klj).\end{aligned}$$

这就完成了证明. □

我们再来看一下置换 σ 与 $\pi\sigma\pi^{-1}$ 的轮换分解的关系. 对于任意一个轮换

$$(i_1 i_2 \cdots i_r),$$

我们来计算

$$\pi(i_1i_2\cdots i_r)\pi^{-1}.$$

设 $\pi(i_k)=j_k$, $k=1,\cdots,r$, 直接验证可知

$$\pi(i_1i_2\cdots i_r)\pi^{-1}(j_k)=j_{k+1},\quad k=1,\cdots,r-1,$$
$$\pi(i_1i_2\cdots i_r)\pi^{-1}(j_r)=j_1,$$

而 $\pi(i_1i_2\cdots i_r)\pi^{-1}$ 保持其余的数不动. 这就是说,

$$\begin{aligned}\pi(i_1i_2\cdots i_r)\pi^{-1}&=(j_1j_2\cdots j_r)\\&=(\pi(i_1)\pi(i_2)\cdots\pi(i_r)).\end{aligned}$$

因之, 当置换 σ 分解成不相交的轮换的乘积时, $\pi\sigma\pi^{-1}$ 的轮换分解就是从 σ 的轮换分解把所有出现的数字 i 都换成 $\pi(i)$ 得到的. 例如,

$$\sigma=(123)(45),$$
$$\pi=\begin{pmatrix}1&2&3&4&5\\5&4&1&3&2\end{pmatrix},$$
$$\pi\sigma\pi^{-1}=(541)(32).$$

定理 9 *交错群 A_n, $n\geq 5$, 是单群.*

证明 设 $H\lhd A_n$, 而且 $H\neq\{e\}$. 我们来证明 $H=A_n$. 由引理, A_n 是由全体 3- 轮换生成, 为了证明 $H=A_n$, 只需要证明 H 包含全体 3- 轮换就行了. 设 $(i_1i_2i_3)$ 与 $(j_1j_2j_3)$ 是任意两个 3- 轮换. 作置换 π, 使

$$\pi(i_k)=j_k,\ k=1,2,3,$$

而 π 在其余数字上的作用适当定义. 因为 $n\geq 5$, 所以在 i_1,i_2,i_3 之外至少还有两个数字 l,m. 如果 π 为偶置换, 就取 $\varphi=\pi$, 如果 π 是奇置换, 就取 $\varphi=\pi(lm)$, 显然有

$$\varphi(i_1i_2i_3)\varphi^{-1}=(j_1j_2j_3).$$

既然 H 是 A_n 的正规子群, 上面的计算说明, 只要 H 包含一个 3- 轮换, H 就包含全部 3- 轮换. 因之, 我们只需要证明 H 至少包含一个 3- 轮换就行了.

对于一个置换 σ, 如果 $\sigma(i)=i$, 那么 i 就称为 σ 的一个 **不动点**. 在正规子群 H 中, 对于所有非单位的置换, 我们取一个不动点个数最多的置换 τ. 因为对换是奇置换, 所以 τ 的不动点的个数不能是 $n-2$, 一定小于或等于 $n-3$. 如果 τ 的不动点个数等于 $n-3$, 那么 τ 就是一个 3- 轮换, 问题就解决了. 下面就来证明, τ 的不动点的个数小于 $n-3$ 是不可能的. 用反证法, 假设 τ 的不动

点的个数小于 $n-3$. 把 τ 分解成不相交轮换的乘积, 按分解式中是否含有长度 ≥ 3 的轮换, 有以下两种可能:

$$\tau = (123\cdots)\cdots \tag{1}$$

$$\tau = (12)(34)\cdots \tag{2}$$

在情况 (1), τ 的不动点的个数一定小于 $n-4$, 因为 $(123j)$ 是奇置换. 无妨设 4, 5 在 τ 下不是不动的. 不论情形 (1) 或情形 (2), 我们取 $\varphi = (345)$, 作 $\varphi\tau\varphi^{-1}$, $\varphi\tau\varphi^{-1} = (124\cdots)\cdots$, 或者 $\varphi\tau\varphi^{-1} = (12)(45)\cdots$. 令 $\tau_1 = \tau^{-1}\varphi\tau\varphi^{-1}$. 在情形 (1), $\tau_1(1) = 1$; 在情形 (2), $\tau_1(1) = 1, \tau_2(2) = 2$. 而在两种情形下, 所有 τ 的不动点仍然是 τ_1 的不动点. 因此不论在哪种情形, τ_1 的不动点都比 τ 的不动点多, 并且 $\tau_1 \neq e$, 这与 τ 的选择矛盾. 这就证明了 τ 一定是一个 3- 轮换. □

这个结果最早是法国天才数学家伽罗瓦 (E. Galois, 1811-1832) 得到的. 根据伽罗瓦理论由这个结果就推出了, 一般五次和五次以上方程不可能有根式解的重要结论.

至于 $n \leq 4$ 的情形, 直接计算即得:

$$\begin{aligned} A_3 =& \{e, (123), (132)\}, \\ A_4 =& \{e, (12)(34), (13)(24), (14)(23), (123), \\ & (132), (124), (142), (134), (143), (234), (243)\}. \end{aligned}$$

A_3 是三阶循环群, 在 A_4 中, 有正规子群

$$H = \{e, (12)(34), (13)(24), (14)(23)\}.$$

而商群 A_4/H 是一三阶循环群.

§4 可解群

上面我们介绍了单群的概念. 对于一个单群 G, 因为它的换位子群 $G^{(1)}$ 是一个正规子群, 所以有 $G^{(1)} = \{e\}$ 或者 $G^{(1)} = G$. $G^{(1)} = \{e\}$ 表明 G 的任意两个元素的换位子都等于 e, 因而 G 是一个交换群. 这就说明, 对于非交换的单群 G 必有 $G^{(1)} = G$.

一般地说, 对于任意一个群 G, 它的换位子群 $G^{(1)}$ 是 G 的一个非平凡的正规子群.

$$G \rhd G^{(1)},$$

再作换位子群 $G^{(1)}$ 的换位子群 $(G^{(1)})^{(1)}$, 记为 $G^{(2)}$. 这样继续下去，令

$$G^{(k)} = (G^{(k-1)})^{(1)}.$$

我们得到一个递降的群列

$$G \rhd G^{(1)} \rhd G^{(2)} \rhd \cdots \rhd G^{(k-1)} \rhd G^{(k)} \rhd \cdots$$

其中每一项 $G^{(k)}$ 都是前一项 $G^{(k-1)}$ 的换位子群. 因而是正规子群. 如果 G 是有限群，那么这样的群列只有两个可能：一是从某个正整数 k 开始有 $G^{(k)} = G^{(k+1)} = \cdots \neq \{e\}$, 一是有个正整数 k 使 $G^{(k)} = \{e\}$.

定义 2 设 G 是一个群. 如果有一正整数 k 使 $G^{(k)} = \{e\}$, 那么 G 称为**可解群**.

显然，可解群包含阿贝尔群作为一个子类，因为对于阿贝尔群 G, 有 $G^{(1)} = \{e\}$.

S_2 是阿贝尔群，因而是可解的.

如 $G = S_3$, 不难验证 $G^{(1)} = \{e, (123), (132)\} = A_3$, $G^{(2)} = A_3^{(1)} = \{e\}$, 因而是可解的.

如 $G = S_4$, 不难验证 $G^{(1)} = A_4$, 而 $G^{(2)} = A_4^{(1)} = \{e, (12)(34), (13)(24), (14)(23)\}$, $G^{(3)} = \{e\}$, 因而也是可解的.

当 $n > 4$, 在 S_n 中任意一个换位子

$$\sigma\tau\sigma^{-1}\tau^{-1}$$

一定是偶置换，因而有

$$S_n^{(1)} < A_n.$$

$S_n^{(1)}$ 是 S_n 的正规子群，当然也是 A_n 的正规子群，且 $S_n^{(1)} \neq \{e\}$(为什么？), 由 A_n 是单群可知

$$S_n^{(1)} = A_n,$$

同时 $S_n^{(2)} = A_n^{(1)} = A_n$. 这就说明，当 $n > 4$ 时， S_n 不可解.

设 G 是一可解群，由定义有正整数 k 使

$$G^{(k)} = \{e\},$$

或者说，有一递降的子群列

$$G = G^{(0)} > G^{(1)} > \cdots > G^{(k)} = \{e\},$$

其中每一个 $G^{(i)}$ 都是前一个 $G^{(i-1)}$ 的正规子群，而且对应的商群

$$G^{(i-1)}/G^{(i)},\ i=1,\cdots,k,$$

都是交换群. 下面我们来证明，这个性质是可解群的一个刻画性质.

定理 10 *群 G 是可解的当且仅当存在一递降的子群列*

$$G=G_0>G_1>\cdots>G_s=\{e\},$$

其中每一个 G_i 是前一个 G_{i-1} 的正规子群，且商群 G_{i-1}/G_i 交换，$i=1,\cdots,s$.

证明 可解群显然具有一个这样的子群列. 反过来，如果群 G 有这样一个子群列，我们来证明 G 可解.

在 §1 的最后我们已经指出，对于 G 的正规子群 N, G/N 交换的充分必要条件为

$$G^{(1)}<N.$$

由 G_0/G_1 交换即得

$$G^{(1)}<G_1,$$

反复利用这个结论，用归纳法不难证明

$$G^k<G_k,\quad k=1,\cdots,s.$$

因为 $G_s=\{e\}$, 所以有 $G^{(s)}=\{e\}$, 这就证明了 G 可解. □

下面再来进一步看看有限可解群的情形.

由 §1 定理 1 我们知道，当 N 是群 G 的正规子群时，商群 G/N 的正规子群与 G 中包含 N 的正规子群是一一对应的. 因之，商群 G/N 是单群的充分必要条件为正规子群 N 不包含在另一个非平凡的正规子群之中，即不存在 G 的正规子群 $N_1, N_1\neq G, N_1\neq N$, 而

$$N<N_1\lhd G.$$

具有这个性质的正规子群称为**极大的**. 这就是说，只要商群 G/N 不是单群，我们总可以找到一个 G 的正规子群 $N_1, N_1\neq G, N_1\neq N$ 使

$$G\rhd N_1\rhd N.$$

设 G 是一有限的可解群. 由定理 10, 有一递降的子群列

$$G=G_0\rhd G_1\cdots\rhd G_k=\{e\},$$

其中商群 G_{i-1}/G_i, $i=1,\cdots,k$, 都是有限交换群. 根据上面的讨论, 只要商群

$$G_{i-1}/G_i$$

不是单群, 我们就可以在 G_{i-1} 与 G_i 之间插入一个子群 G_i', $G_i'\neq G_{i-1}$, $G_i'\neq G_i$ 使

$$G_{i-1}\rhd G_i'\rhd G_i,$$

其中商群 G_i'/G_i 为交换群 G_{i-1}/G_i 的子群, 商群 G_{i-1}/G_i' 同构于交换群 G_{i-1}/G_i 的商群

$$(G_{i-1}/G_i)/(G_i'/G_i),$$

因而它们都仍然是交换群.

因为 G 是有限群, 所以上面这种递降子群列的长度 k 是有限的 $(k\leq|G|)$. 这就是说, 经过若干次的插入之后, 我们总可以达到一个递降子群列

$$G=H_0>H_1\rhd\cdots\rhd H_t=\{e\},$$

它不能再插入新的项, 换句话说, 每一个商群

$$H_{i-1}/H_i,\ \ i=1,\cdots,t,$$

都是交换的单群, 也就是素数阶的循环群.

这就证明了

定理 11 *有限群 G 是可解的充分必要条件为存在一个递降的子群列*

$$G=H_0>H_1\rhd\cdots\rhd H_t=\{e\},$$

其中商群 H_{i-1}/H_i, $i=1,\cdots,t$. 都是素数阶的循环群. □

应该指出, 对于有限可解群 G, 定理 11 中的子群列 $H_1,\cdots,H_t$ 并不是唯一的.

令商群

$$H_{i-1}/H_i$$

的阶分别为素数 p_i, $i=1,\cdots,t$. 显然有

$$|G|=p_1\cdots p_t.$$

这就说明, 定理 11 中的子群列虽然不唯一, 但是长度 t 就等于 $|G|$ 的素因子的个数 (重复的重复计算), 是唯一决定的, 同时素数组

$$p_1,\cdots,p_t$$

是唯一决定的.

§5 群的自同构群

一个群到它自身的同构映射称为**自同构映射**,或简称**自同构**. 由同构关系的反身性, 对称性与传递性立即看出, 一个群的全部自同构在变换的乘法下成一个群, 称为**自同构群**. 群 G 的自同构群记为 $\mathrm{Aut}(G)$.

作为例子, 我们来看看循环群的自同构群. 设 G 为一无限循环群 $G=\langle g\rangle$. σ 是 G 的自同构. 显然, σ 的作用完全被 G 的生成元 g 的象 $\sigma(g)$ 所决定. 因为 σ 是满的, 即 $\sigma(G)=G$, 所以 $\sigma(g)$ 还是 G 的一个生成元. 由此可见, $\sigma(g)=g$ 或者 $\sigma(g)=g^{-1}$. 当 $\sigma(g)=g$, σ 就是单位自同构 e. 容易验证, $\sigma(g)=g^{-1}$, 一般地, $\sigma(g^x)=g^{-x}$ 是 G 的一个自同构. 因之

$$\mathrm{Aut}(G)=\{e,\sigma\},\ \text{其中}\ \sigma^2=e.$$

设 G 为一有限循环群, $G=\langle g\rangle$, 其中 $g^n=e$, 即 $|G|=n$, σ 是 G 的一个自同构. 同样地, $\sigma(g)$ 一定是 G 的生成元. 我们知道, G 的生成元是 g^t, 其中 $(t,n)=1$, 因之, G 的每个自同构决定一正整数 $t, 0<t<n, (t,n)=1$, 即 $\sigma(g)=g^t$. 如果 $\sigma(g)=g^t, \tau(g)=g^s$, 那么 $\tau\sigma(g)=\tau(g^t)=g^{st}$. 在整数模 n 的环 $\mathbf{Z}/n\mathbf{Z}$ 中, 所有与 n 互素的剩余类对于乘法组成一个群, 记这个群为 $\mathbf{Z}/n\mathbf{Z}^*$. 以上分析表明, 当 $G=\langle g\rangle$ 为 n 阶循环群时,

$$\mathrm{Aut}(G)\cong \mathbf{Z}/n\mathbf{Z}^*.$$

设 G 为任意一个群, $a\in G$ 为一固定元素. 我们定义 $\sigma_a: G\to G$ 为

$$\sigma_a(x)=axa^{-1},\quad x\in G.$$

由 $\sigma_a\sigma_{a^{-1}}(x)=\sigma_{a^{-1}}\sigma_a(x)=x$ 可知, σ_a 是一个一一对应. 显然

$$\sigma_a(xy)=axya^{-1}=(axa^{-1})(aya^{-1})=\sigma_a(x)\sigma_a(y).$$

因之, 对所有的 $a\in G, \sigma_a$ 是 G 的自同构. 这样由 G 中元素引起的自同构称为**内自同构**. 容易验证,

$$\sigma_a\sigma_b=\sigma_{ab}.$$

这就是说, $a\mapsto\sigma_a$ 给出了群 G 到 $\mathrm{Aut}(G)$ 的一个同态. G 的同态象就是 G 的全体内自同构, 它们组成 $\mathrm{Aut}(G)$ 的一个子群, 这个子群记为 $\mathrm{In}(G)$, 称为 G 的**内自同构群**. 我们用 $f: G\to\mathrm{In}(G)$ 代表同态 $a\mapsto\sigma_a$. 下面来考察一下 f 的核.

如果 $a\in\ker(f)$, 那么

$$\sigma_a(x)=axa^{-1}=x,$$

对所有的 $x \in G$. 这就是说，a 与 G 中所有元素可交换. 反过来，如果 $a \in G$ 与 G 中所有元素可交换，那么 $\sigma_a(x) = axa^{-1} = x$, 即 $\sigma_a = e$.

在任意一个群 G 中，所有与 G 的全体元素可交换的元素的集合称为 G 的**中心**, 记为 $Z(G)$. 以上讨论说明，群 G 的中心 $Z(G)$ 就等于 $\ker(f)$, $Z(G)$ 是 G 的正规子群，而且根据同态基本定理，我们有

$$G/Z(G) \cong \mathrm{In}(G).$$

定理 12 设 G 是任意一个群. 我们有

$$\mathrm{In}(G) \lhd \mathrm{Aut}(G).$$

证明 设 $\sigma_a \in \mathrm{In}(G), \tau \in \mathrm{Aut}(G)$. 于是

$$\begin{aligned}\tau\sigma_a\tau^{-1}(x) &= \tau\sigma_a(\tau^{-1}(x)) \\ &= \tau(a\tau^{-1}(x)a^{-1}) \\ &= \tau(a)x\tau(a)^{-1} \\ &= \sigma_{\tau(a)}(x),\end{aligned}$$

即

$$\tau\sigma_a\tau^{-1} = \sigma_{\tau(a)} \in \mathrm{In}(G).$$

这就证明了，$\mathrm{In}(G)$ 是 $\mathrm{Aut}(G)$ 的正规子群. □

自同构群对于内自同构群的商群

$$\mathrm{Aut}(G)/\mathrm{In}(G)$$

称为群 G 的**外自同构群**.

由上面的讨论，当群 G 的中心 $Z(G) = \{e\}$ 时，我们有

$$G \cong \mathrm{In}(G).$$

在这个情形下，我们可以认为 G 的自同构群包含 G 作为它的子群.

定理 13 如果 $Z(G) = \{e\}$, 那么 G 的自同构群 $\mathrm{Aut}(G)$ 的中心也只含有单位元素.

证明 我们来证明，在定理的条件下，与全体内自同构交换的自同构一定是单位自同构.

设 $a \in G$, 与 a 对应的内自同构 $\sigma_a \in \mathrm{In}(G), \tau \in \mathrm{Aut}(G)$. 由定理 12 的证明，我们有

$$\tau\sigma_a\tau^{-1} = \sigma_{\tau(a)}.$$

如果 $\tau\sigma_a = \sigma_a\tau$, 那么 $\sigma_a = \sigma_{\tau(a)}$, 即

$$\tau(a)a^{-1} \in Z(G).$$

由 $Z(G) = \{e\}$, 即得

$$\tau(a)a^{-1} = e,$$

$$\tau(a) = a, \text{ 对所有的 } a \in G.$$

这就是说, τ 是单位自同构, 因而

$$Z(\mathrm{Aut}(G)) = \{e\}. \quad \square$$

这个结果说明, 从一个中心是单位的群 G 出发, 作它的自同构群 $\mathrm{Aut}(G)$, 我们有

$$G < \mathrm{Aut}(G), \text{ 且 } Z(\mathrm{Aut}(G)) = \{e\}.$$

于是我们再作 $\mathrm{Aut}(G)$ 的自同构群, 这样一层一层地上去就得到一串群

$$G < \mathrm{Aut}(G) < \mathrm{Aut}(\mathrm{Aut}(G)) < \cdots$$

一个自然提出的问题是: 这一串群可不可能无限地作下去? 维兰特 (Wielandt) 在 1951 年解决了这个问题, 即从任意一个中心为单位的有限群 G 出发, 一步一步地作群的自同构群, 有限步之后一定终止, 换句话说, 有限步之后我们一定得到一个群, 它的自同构都是内自同构. 一个中心为单位且自同构全是内自同构的群称为**完全群**. 维兰特的结果就是, 从任意一个中心为单位的有限群出发, 不断作自同构群, 有限步之后一定得到一个完全群.

§6 群在一集合上的作用

设 X 是任意一个集合 (非空的), 我们知道, 集合 X 的全体到自身的一一对应组成一个群 $S(X)$, $S(X)$ 的子群称为集合 X 的变换群. 从历史的发展看, 人们最早研究的都是某一集合上的变换群. 直到现在, 各种类型的变换群的研究仍是群论的一个重要部分. 抽象群的概念正是从变换群来的. 在群论的发展中, 一方面是把抽象群论中得到的结果应用到变换群上, 另一方面也常常利用变换群来研究抽象群的性质. 以前讲过的凯莱定理就是建立这二者的联系. 这一节就是要引入一个适当广泛的定义来体现抽象群与变换群的联系.

定义 3 设 G 是一个群, X 是一非空集合. 如果给了一个映射 $f: G \times X \to X$, 适合条件: 对所有的 $g_1, g_2 \in G, x \in X$,

1) $f(e,x)=x$;

2) $f(g_1g_2,x)=f(g_1,f(g_2,x))$;

那么我们就说， f 决定了 **群 G 在集合 X 上的作用**.

在不需要明确指出映射 f 的情况下，我们常常把 $f(g,x)$ 简写成 $g(x)$. 按这个写法，定义中的条件就可以写成

1) $e(x)=x$,

2) $g_1(g_2(x))=g_1g_2(x)$.

根据定义，如果群 G 作用在集合 X 上，那么 G 的每个元素 g 都对应集合 X 的一个到自身的映射 $\sigma_g: x\mapsto g(x)$. 由定义中的条件，我们有

$$g^{-1}(g(x))=g(g^{-1}(x))=e(x)=x,$$

这就说明， G 中每个元素 g 对应的映射 σ_g 都是集合 X 的到自身的一一对应，即

$$\sigma_g\in S(X),$$

且 $\sigma_g^{-1}=\sigma_{g^{-1}}$. 显然， $g\mapsto\sigma_g$ 是群 G 到群 $S(X)$ 的一个同态映射.

反过来，如果给了一个同态映射 ψ

$$\psi: G\to S(X),$$

并且定义

$$g(x)=\psi(g)(x),\ \text{对 } g\in G, x\in X,$$

那么就决定了群 G 在集合 X 上的作用. 由此，我们也可以用群 G 到 $S(X)$ 的同态来定义群 G 在集合 X 上的作用. 这两种说法是一致的.

下面来看几个例子.

例 1 设 G 是一个群，取 $X=G$. 定义

$$g(x)=gx,\ \text{对 } g,x\in G.$$

这就给出了一个群在集合 G 上的作用. 这就是我们以前所谓的左平移.

例 2 设 G 是一个群，取 $X=G$. 定义

$$g(x)=gxg^{-1},\ \text{对 } g,x\in G.$$

这就是通常所谓的群上的 **共轭变换**. 在共轭变换下，元素 gxg^{-1} 称为与元素 x **共轭**. 同样，子群 gHg^{-1} 称为与子群 H 共轭. 它们都是等价关系.

例 3 设 G 是一个群，$H < G, G$ 按子群 H 分成左陪集 $\{xH, x \in G\}$，令 X 为全体左陪集所成的集合．定义

$$g(xH) = gxH,\ g, x \in G.$$

这就决定了群 G 在集合 X 上的作用．由左陪集构成的集合通常称为群 G 的一个 **齐性空间**．

当群 G 作用在集合 X 上，完全可能 G 中不同的元素在 X 上引起相同的映射，换句话说，同态 $g \mapsto \sigma_g$ 不一定是单射．在上面的例 2 中，如果群 G 的中心包含单位元素以外的元素，那么显然，中心的元素全对应 G 的恒同映射．如果同态 $g \mapsto \sigma_g$ 是单射，那么我们就说，群 G 在集合 X 上的作用是 **如实的**．或者说，群 G 是如实地作用在集合 X 上．例 1 中的作用就是如实的，而例 2，例 3 就不一定是如实的．

定义 4 设 G 是一个群，X, X' 是两个非空集合，G 作用在 X 上，同时 G 也作用在 X' 上．如果有一个一一对应 $\varphi: X \to X'$ 使

$$\varphi(g(x)) = g(\varphi(x)),$$

那么这两个作用就称为 **等价的**．

从抽象的观点看，两个等价的作用可以不加区别．

以前我们定义过 G 上的右平移，即对于 $g, x \in G, g(x) = xg^{-1}$．在 G 上，定义

$$\varphi(x) = x^{-1},\ \ x \in G.$$

由

$$\varphi(gx) = (gx)^{-1} = x^{-1}g^{-1} = \varphi(x)g^{-1}$$

立即看出，左平移与右平移是等价的．

设群 G 作用在非空集合 X 上，在集合 X 上我们来定义一等价关系 “$\sim$”．对于 $x, y \in X$，如果在 G 中有一个元素 g 使得 $y = g(x)$，那么就说 $x \sim y$(读为 x 等价于 y)．容易证明，关系 “$x \sim y$” 确实是一个等价关系 (证明留给读者)．在这个等价关系下，集合 X 的元素被分成等价类．这样分成的等价类称为 **轨道**．由定义可知，包含元素 x 的轨道就是子集合

$$O_x = \{g(x) \mid g \in G\}.$$

显然，集合 X 就是全部不同的轨道的并，即

$$X = \bigcup_x O_x，\text{其中 } x \text{ 取遍不同轨道的代表}.$$

轨道 O_x 也可能只包含单个的元素 x, 这就是说, 对于所有的 $g \in G$ 都有

$$g(x) = x.$$

这样的元素 x 称为 G 的**不动元素**. 在上面的例 2 中, 对于 $g, x \in G, g(x) = gxg^{-1}$, 如果 $x \in Z(G)$, 那么显然 $O_x = \{x\}$; 反过来, 由 $O_x = \{x\}$ 可知 $x \in Z(G)$.

也有可能集合 X 本身就是一个轨道, 这就是说, 对于任意的 $x, y \in X$, 都有一个元素 $g \in G$, 使 $y = g(x)$. 在这个情况, 我们说, 群 G 在集合 X 上的作用是 **传递的**. 不难看出, 上面的例 1 与例 3 都是传递的情形.

设 V 是域 F 上的一个 n 维线性空间, $GL_n(F)$ 是域 F 上全体 $n \times n$ 可逆矩阵组成的一般线性群. 在 V 中取定一组基后, 每个可逆矩阵 $A \in GL_n(F)$ 就对应 V 的一个可逆线性变换 $\boldsymbol{A}$. 显然, 定义 $A(x) = \boldsymbol{A}(x)$ 就给出了 $GL_n(F)$ 在 V 上的作用. 零向量是 $GL_n(F)$ 的一个不动元素; 因为任意两个非零向量都可以用可逆线性变换互变, 所以全体非零向量组成一个轨道. 由此可知, V 是两个轨道的并,

$$V = \{0\} \cup \{\alpha \in V \mid \alpha \neq 0\}.$$

设群 G 作用在集合 X 上, 对于集合 X 中任意一个元素 x, 容易看出集合

$$\{g \in G \mid g(x) = x\}$$

是 G 的一个子群, 我们用 H_x 表示这个子群, 它称为元素 x 的 **稳定子群**.

定理 14 设群 G 作用在集合 X 上, $x \in X, O_x$ 是包含 x 的轨道, H_x 是 x 的稳定子群. 于是群 G 在集合 O_x 上的作用与群 G 在齐性空间 G/H_x 上的作用等价.

证明 首先, 由轨道的定义, 对于任意元素 $y \in O_x$, 任意的 $g \in G$, 显然有

$$g(y) \in O_x.$$

因之, 考虑 G 在 O_x 上的作用是有意义的.

对于任意一个左陪集 aH_x, 任意元素 $g \in aH_x$, 显然有

$$g(x) = a(x).$$

这就是说, 同一个左陪集中不同的元素把 x 变到同一个元素. 反过来, 如果 $g_1, g_2 \in G$ 使

$$g_1(x) = g_2(x),$$

那么 $g_2^{-1}g_1(x) = x$, 即 $g_2^{-1}g_1 \in H_x$, 因而 g_1, g_2 属于同一个左陪集. 我们定义映射

$$\psi : G/H_x \to O_x$$

为

$$\psi(aH_x) = a(x).$$

以上讨论表明，映射 ψ 是集合 G/H_x 到 O_x 的一个一一对应.（为什么 ψ 是满的？）

显然有

$$\psi(gaH_x) = ga(x) = g(\psi(aH_x)),$$

因而 G 在 O_x 上的作用与 G 在齐性空间 G/H_x 上的作用等价. □

推论 1 设群 G 在集合 X 上的作用是传递的，$x \in X, H_x$ 是元素 x 的稳定子群. 于是 G 在 X 上的作用与 G 在齐性空间 G/H_x 上的作用等价.

证明 显然. □

推论 1 表明，对于任意一个群 G, G 的传递作用的集合的研究就归结为 G 的齐性空间的研究.

推论 2 设 G 是有限群，G 作用在集合 X 上. 于是任意一个轨道 O_x 包含有限多个元素，且包含元素的个数是群 G 的阶的因子.

证明 设 H_x 是元素 x 的稳定子群. 我们知道

$$|O_x| = |G/H_x|,$$

这就证明了所要的结论. □

一个有限群 G 称为 p- 群(p 为素数), 如果 G 的阶是素数 p 的方幂，即

$$|G| = p^k,\ k \geq 1.$$

推论 3 设有限群 G 作用在一个有限集合 X 上. 如果 G 是 p- 群，$|X| = n$, $(n,p) = 1$, 那么 X 中必有不动元素.

证明 设 $O_{x_1}, O_{x_2}, \cdots, O_{x_m}$ 是集合 X 的全部轨道. 我们知道，x_i 是不动元素的充分必要条件是 $|O_{x_i}| = 1$. 如果 x_i 不是不动元素，那么由推论 2,$|O_{x_i}| = p^l, l \geq 1$. 因为

$$n = |X| = \sum_{i=1}^{m} |O_{x_i}|,$$

所以由 $(n,p) = 1$ 可知必有 x_i 使 $|O_{x_i}| = 1$. □

在上面的证明中我们看到，只要 $|O_{x_i}| > 1$ 就有 $p \mid |O_{x_i}|$. 因之进一步有

推论 4 设 p- 群 G 作用在一个有限集合 X 上，$|X| = n$. 如果 t 为 X 中不动元素的个数，那么

$$t \equiv n \pmod{p}.$$

证明 由

$$n = t + \sum_{|O_x|>1} |O_x|$$

即得所要的结论. □

推论 5 *p- 群必有非平凡的中心.*

证明 设 G 为一 p- 群, 考虑 G 在 G 上的共轭变换. 在这个情况下, 我们知道只有中心的元素才构成单个元素的轨道. 令

$$t = |Z(G)|.$$

由推论 4 即得

$$t \equiv 0 \pmod{p}.$$

因为 $t \geq 1$, 所以一定有 $t > 1$. □

顺便说一下, 当 G 在 G 上的作用是共轭变换时, 包含 G 中元素 x 的轨道称为 x 所在的 **共轭类**, 记为 $C(x)$. 对于有限群 G, 我们有

$$|C(x)| = |G/H_x|,$$

其中 H_x 是 x 的稳定子群. 由共轭变换的定义, 显然

$$H_x = \{g \in G \mid gx = xg\},$$

即 H_x 由全部与 x 可交换的元素所组成. 这个子群称为元素 x 的 **中心化子**, 记为 $Z(x)$. 明显地, $Z(x) = G$ 当且仅当 $x \in Z(G)$. 因之, 对于有限群 G, 我们有

$$|G| = |Z(G)| + \sum_x [G : Z(x)],$$

其中 x 取遍非中心元素的共轭类的代表. 这个公式在有限群的讨论中是有用的.

最后再说明一点. 定理 14 断言群 G 在轨道 O_x 上的作用与 G 在齐性空间 G/H_x 上的作用等价, 这里 x 是轨道 O_x 中任意一个元素. 由此立即推出, 对于 $x, y \in O_x$, 齐性空间 G/H_x 与 G/H_y 是等价的. 实际上我们可以证明

定理 15 *设群 G 作用在集合 X 上, $x, y \in X$. 如果有 $g_0 \in G$ 使 $y = g_0 x$, 那么 $H_y = g_0 H_x g_0^{-1}$.*

证明 对于 $g \in H_x$, 即 $g(x) = x$, 我们有

$$\begin{aligned}(g_0 g g_0^{-1})(y) &= g_0 g g_0^{-1}(g_0(x)) \\ &= g_0 g(x) = g_0(x) = y,\end{aligned}$$

这就是说， $g_0 g g_0^{-1} \in H_y$, 即

$$g_0 H_x g_0^{-1} < H_y.$$

同样可以证明

$$H_y < g_0 H_x g_0^{-1}. \quad \square$$

§7 西罗定理

我们知道，对于有限群，每个子群的阶都是群的阶的因子. 很自然地要问，对于群的阶的任何一个因子，是否都存在一个子群，以这个因子为阶. 不难举出例子，这样一个一般形式的结论是不成立的. 譬如 4 次交错群 A_4 的阶是 12, 它有 2 阶，3 阶与 4 阶子群，但是没有 6 阶子群; 又如我们已经证明，当 $n \geq 5$ 时，A_n 是单群，不难证明，在有限群中，任何一个指数为 2 的子群一定正规，由此可见，在 A_n $(n \geq 5)$ 中，不存在阶为 $\frac{1}{4}n!$ 的子群. 在这一节我们将部分地给出这个问题的肯定回答. 具体地说，我们将证明，当因子是素数方幂时，这样的子群是存在的，同时讨论这种子群的一些性质. 以下得到的几条主要定理通常称为西罗定理.

定理 16 **(西罗 (Sylow) 第一定理)** *设 G 是一有限群，p 是素数. 如果 $p^k \mid |G|$, $k \geq 0$, 那么 G 中一定有一个阶为 p^k 的子群.*

设 $|G| = n = p^l m$, $(p, m) = 1$. 于是由定理的条件有 $k \leq l$. 下面先证一个引理.

引理 *设 $n = p^l m$, $(p, m) = 1, k \leq l$, $C_n^{p^k}$ 是组合数. 于是 $p^{l-k} \mid C_n^{p^k}$, 但 $p^{l-k+1} \nmid C_n^{p^k}$.*

证明 我们知道

$$C_n^{p^k} = \frac{n(n-1)\cdots(n-p^k+1)}{p^k(p^k-1)\cdots 1}.$$

为了证明所要的结论，我们来看一下分子与分母的各个因子中所含的 p 的方幂. 容易看出，$n - i = p^l m - i$ 与 $p^k - i$, 在 $0 < i < p^k$ 的情形下，包含的 p 的方幂是一样的. 事实上，如果 $i = p^t \cdot i'$, $(p, i') = 1$, $0 \leq t < k$, 那么有

$$\begin{aligned} p^l m - p^t \cdot i' &= p^t(p^{l-t}m - i'), \\ p^k - p^t \cdot i' &= p^t(p^{k-t} - i'). \end{aligned}$$

显然，$(p, p^{l-t}m - i') = 1, (p, p^{k-t} - i') = 1$. 这就说明，分数

$$r = \frac{(n-1)\cdots(n-p^k+1)}{(p^k-1)\cdots 1}$$

在消去分子与分母中含有的 p 的因子之后是一个分子与分母全与 p 互素的分数. 于是

$$C_n^{p^k} = p^{l-k} \cdot m \cdot r,$$

这就证明了引理.

定理的证明: 令 X 是 G 中全部含有 p^k 个元素的子集合的集合. 显然 $|X| = C_n^{p^k}$. 对于 X 中元素 A, 定义

$$g(A) = gA,\ g \in G,$$

这就给出了群 G 在集合 X 上的作用. 我们知道, 集合 X 可以分解成全部轨道的并, 即

$$|X| = \sum |O_A|.$$

因为 $p^{l-k+1} \nmid |X|$, 所以, 至少有一个轨道, 譬如说 O_A, 有 $p^{l-k+1} \nmid |O_A|$. 令 H_A 是 A 的稳定子群, 由 $|O_A| = |G/H_A|$ 可知

$$p^k \mid |H_A|.$$

另一方面, 取 $a \in A$, 既然 H_A 是 A 的稳定子群, 必然有

$$H_A a \subset A,$$

即

$$|H_A a| = |H_A| \leq |A| = p^k.$$

因之 $|H_A| = p^k, H_A$ 就是一个阶为 p^k 的子群. □

特别地, 当 $|G| = p^l \cdot m, (p, m) = 1$ 时, G 有阶为 p^l 的子群. 阶为 p^l 的子群称为 G 的 **西罗 p- 子群**.

定理 17 **(西罗第二定理)** 设有限群 G 的阶为 $p^l \cdot m$, 其中 p 为素数, $(p, m) = 1$, P 为 G 的一个西罗 p- 子群. 于是 G 的任意一个阶为 p^k $(k \leq l)$ 的子群 H 一定包含在一个与 P 共轭的西罗 p- 子群中.

证明 令 X 为 P 的左陪集所成的集合, 定义 H 在 X 上的作用为:

$$h(gP) = hgP, \quad 其中\ h \in H, g \in G.$$

我们知道, $|X| = m, |H| = p^k$. 由定理 14 的推论 3,X 有一不动元素, 即有一左陪集 gP 使

$$HgP \subset gP.$$

由此即得

$$H \subset gPg^{-1}. \quad \square$$

特别地，当 H 也是一个西罗 p- 子群时，我们有

推论 1 在有限群中，任意两个西罗 p- 子群都互相共轭. $\square$

由推论 1 可以知道，一个有限群 G 有唯一的西罗 p- 子群 P 的充分必要条件是 P 在 G 中正规.

对于群 G 中任一子群 H, 我们定义

$$N(H) = \{g \in G \mid gHg^{-1} = H\}.$$

显然，$N(H)$ 是一子群且 $N(H) \supset H$. $N(H)$ 称为子群 H 的**正规化子**. 由定义立即推出

$$H \lhd N(H).$$

推论 2 设 G 为一有限群，P 是 G 的一个西罗 p- 子群. 于是 $N(N(P)) = N(P)$, $N(P)$ 中不可能包含 G 的另一个西罗 p- 子群.

证明 既然 P 是 G 的一个西罗 p- 子群，P 当然也是 $N(P)$ 的西罗 p- 子群. 由 $P \lhd N(P)$ 可知 P 是 $N(P)$ 中唯一的一个西罗 p- 子群, 因而 $N(P)$ 不可能包含 G 的另一个西罗 p- 子群.

如果 $g \in N(N(P))$, 即

$$gN(P)g^{-1} = N(P),$$

那么 gPg^{-1} 也是 $N(P)$ 的西罗 p- 子群，因而

$$gPg^{-1} = P.$$

这就是说，$g \in N(P)$, $N(N(P)) \subset N(P)$. 显然，$N(N(P)) \supset N(P)$, 于是

$$N(N(P)) = N(P). \quad \square$$

推论 3 设 G 为一有限群，p 为一素数，$p \mid |G|$. 于是 G 中全部西罗 p- 子群的个数是 $|G|$ 的因子.

证明 令 X 是 G 中全部西罗 p- 子群所成的集合. 我们定义 G 在 X 上的作用为:

$$g(Q) = gQg^{-1}, \quad 对于\ g \in G, Q \in X.$$

根据定理 17 的推论 1,G 在 X 上的作用是传递的. 取 $P \in X$, 显然 P 的稳定子群就是 $N(P)$, 于是

$$|X| = [G : N(P)],$$

这就证明了所要的结论. □

定理 18 (西罗第三定理) 设 G 为一有限群, p 为一素数, $p||G|$, k 是 G 中全部西罗 p- 子群的个数. 于是 $k \equiv 1 \pmod{p}$.

证明 令 X 是 G 中全部西罗 p- 子群所成的集合, P 是 G 的一个西罗 p- 子群. 定义 P 在 X 上的作用为:

$$g(Q) = gQg^{-1}, \text{对于 } g \in P, Q \in X.$$

由定理 17 的推论 2, 我们知道, P 是 X 中唯一的一个不动元素. 再利用定理 14 的推论 4 即得

$$k \equiv 1 \pmod{p}. \quad \square$$

结合上面的推论 3, 我们有

推论 设有限群 G 的阶是 $p^l \cdot m$, 其中 $(p,m) = 1$, p 是素数. 于是 G 的西罗 p- 子群的个数是 m 的因子.

证明 显然. □

作为这一节的结束, 我们来看一个例子来说明如何应用上面的结果来解决群论的问题.

设有限群 G 的阶是 72. $72 = 2^3 \cdot 3^2$. G 的西罗 3- 子群的个数是 $1 + 3t$, 由 $(1 + 3t)|8$ 可知 $t = 0$ 或 $t = 1$. 如果 $t = 0$, G 有唯一的一个 9 阶子群. 这个子群是正规的, 如果 $t = 1$, G 有 4 个 9 阶子群 P_1, P_2, P_3, P_4. 考虑 G 在集合

$$X = \{P_1, P_2, P_3, P_4\}$$

上的共轭变换. G 的每个元素在 X 上引起一个 4 次置换. 这就给出了一个同态

$$\varphi : G \to S_4.$$

因为 $72 > 24 = |S_4|$, 而且 $\varphi(G) \neq \{e\}$, 所以 $\ker(\varphi)$ 非平凡 ($\ker(\varphi)$ 的阶至少是 3). 综合以上两种情形, G 必有非平凡的正规子群. 这就说明, 阶为 72 的群一定不是单群.

§8 群的直和

现在我们来介绍一种由已知群构造新的群的方法. 先看两个群的情形.

设 G_1, G_2 是两个群, 考虑集合

$$G_1 \times G_2.$$

对于 $G_1 \times G_2$ 中任意两个元素 $(a_1,b_1),(a_2,b_2)$ 我们定义乘法为:

$$(a_1,b_1)(a_2,b_2)=(a_1a_2,b_1b_2),$$

其中第一个分量是作 G_1 的乘法，第二个分量是作 G_2 的乘法. 由于群 G_1,G_2 的乘法有结合律，所以新定义的乘法显然也适合结合律.

令 e_1,e_2 分别是群 G_1、G_2 的单位元素，于是对所有的 $(a,b)\in G_1\times G_2$ 有

$$\begin{aligned}(a,b)(e_1,e_2)&=(e_1,e_2)(a,b)\\&=(a,b),\end{aligned}$$

即 $G_1\times G_2$ 在新定义的乘法下有单位元素 (e_1,e_2). 对于所有的 $(a,b)\in G_1\times G_2$ 有

$$(a,b)(a^{-1},b^{-1})=(e_1,e_2),$$

即 $G_1\times G_2$ 中每个元素有逆元素.

以上讨论表明，$G_1\times G_2$ 在所定义的乘法下成一群. 我们称这个群为群 G_1 与 G_2 的 **直和**, 记为

$$G_1\oplus G_2.$$

显然，直和 $G_1\oplus G_2$ 的结构完全被群 G_1、G_2 的结构所决定.

当 G_1,G_2 是有限群时，$|G_1|=n_1,|G_2|=n_2$，于是 $G_1\oplus G_2$ 也是有限群，且

$$|G_1\oplus G_2|=n_1n_2.$$

在 $G_1\oplus G_2$ 中令

$$\begin{aligned}\overline{G_1}&=\{(a,e_2),a\in G_1\},\\\overline{G_2}&=\{(e_1,b),b\in G_2\}.\end{aligned}$$

容易验证，$\overline{G_1}$ 与 $\overline{G_2}$ 都是 $G_1\oplus G_2$ 的子群. 显然映射 $a\mapsto(a,e_2)$ 是 G_1 到 $\overline{G_1}$ 的一个同构，同样，映射 $b\mapsto(e_1,b)$ 是 G_2 到 $\overline{G_2}$ 的一个同构. 这就是说，G_1,G_2 分别与子群 $\overline{G_1},\overline{G_2}$ 同构.

对于任意的 $(a_1,b_1)\in G_1\oplus G_2$, 有

$$\begin{aligned}&(a_1^{-1},b_1^{-1})(a,e_2)(a_1,b_1)\\&\quad=(a_1^{-1}aa_1,b_1^{-1}b_1)\\&\quad=(a_1^{-1}aa_1,e_2)\in\overline{G_1},\\&(a_1^{-1},b_1^{-1})(e_1,b)(a_1,b_1)\\&\quad=(a_1^{-1}a_1,b_1^{-1}bb_1)\\&\quad=(e_1,b_1^{-1}bb_1)\in\overline{G_2}.\end{aligned}$$

这就说明，$\overline{G_1},\overline{G_2}$ 都是 $G_1\oplus G_2$ 的正规子群.

对 $G_1\oplus G_2$ 中任意元素 $x=(a,b)$, 有

$$x=(a,b)=(a,e_2)(e_1,b),$$

其中 $x_1=(a,e_2)\in\overline{G_1},x_2=(e_1,b)\in\overline{G_2}$. 即

$$x=x_1x_2,\text{ 其中 } x_1\in\overline{G_1},x_2\in\overline{G_2}.$$

这就是说，直和 $G_1\oplus G_2$ 中的每个元素都可以分解成 $\overline{G_1}$ 与 $\overline{G_2}$ 中元素的乘积. 不难验证，这样的分解式是唯一的.

直和的定义不难推广到多个群的情形. 设 $G_1,\cdots,G_s$ 是 s 个群，考虑集合

$$G_1\times G_2\times\cdots\times G_s.$$

对于其中任意两个元素 $(a_1,\cdots,a_s)$ 与 $(b_1,\cdots,b_s)$ 还是按分量来定义乘法

$$\begin{aligned}&(a_1,\cdots,a_s)(b_1,\cdots,b_s)\\&=(a_1b_1,\cdots,a_sb_s),\end{aligned}$$

其中 $a_i,b_i\in G_i$, $i=1,\cdots,s$.

容易验证，$G_1\times\cdots\times G_s$ 在这样定义的乘法下成一群，它称为群 $G_1,\cdots,G_s$ 的直和，记为

$$G_1\oplus\cdots\oplus G_s.$$

与两个群的情形一样，定义

$$\overline{G_i}=\{(e_1,\cdots,e_{i-1},a_i,e_{i+1},\cdots,e_s),a_i\in G_i\},\quad i=1,\cdots,s,$$

其中 e_i 为群 G_i 的单位元素. 同样地，每个 $\overline{G_i}$ 都是直和 $G_1\oplus\cdots\oplus G_s$ 的正规子群且与 G_i 同构.

对于 $G_1\oplus\cdots\oplus G_s$ 中任意一个元素，

$$x=(a_1,\cdots,a_s).$$

令 $x_i=(e_1,\cdots,e_{i-1},a_i,e_{i+1},\cdots,e_s)$, $i=1,\cdots,s$. $x_i\in\overline{G_i}$ 显然有

$$x=x_1\cdots x_s,$$

即直和 $G_1\oplus\cdots\oplus G_s$ 中的每个元素都能分解成正规子群 $\overline{G_1},\cdots,\overline{G_s}$ 的元素的乘积. 容易看出，这样的分解式是唯一的.

我们知道, 直和 $G_1\oplus\cdots\oplus G_s$ 的结构完全被群 $G_1,\cdots,G_s$ 的结构所决定. 因此, 如果一个群能够分解成某一些群的直和, 那么这个群的研究就可以归结为另一些群 (一般说来, 它们比原来的群简单些) 的研究. 下面就来讨论, 在什么条件下, 一个群能够分解成一些群的直和.

定理 19 设 $N_1,\cdots,N_s$ 是群 G 的正规子群, 如果

1) $G=N_1,\cdots,N_s$;

2) 对于 G 中任意一个元素 x, 表示式 $x=x_1\cdots x_s$, 其中 $x_i\in N_i$, $i=1,\cdots,s$, 是唯一的,

那么

$$G\cong N_1\oplus\cdots\oplus N_s.$$

证明 由表示式

$$x=x_1\cdots x_s,\ x_i\in N_i,\quad i=1,\cdots,s$$

的唯一性我们可以在 G 与 $N_1\oplus\cdots\oplus N_s$ 之间建立一个一一对应, 即

$$x=x_1\cdots x_s\mapsto(x_1,\cdots,x_s).$$

下面就是要证明它是一个同构映射.

先由表示式的唯一性我们来证明

$$N_i\cap N_j=\{e\},\quad 当\ i\neq j.$$

事实上, 如果 $x\in N_i\cap N_j$, 但 $x\neq e$, 那么 x 就要有两种不同的表示式

$$x=e\cdots e\underset{\text{第}i\text{位}}{x}e\cdots e=e\cdots e\underset{\text{第}j\text{位}}{x}e\cdots e,$$

这就证明了 $N_i\cap N_j=\{e\}$, 当 $i\neq j$.

由此我们立即可以证明, 对于任意两个不同的正规子群 N_i 与 N_j, 它们的元素必两两交换, 即对于任意的 $x_i\in N_i, x_j\in N_j$ 有

$$x_ix_j=x_jx_i.$$

为此我们来看元素

$$x_ix_jx_i^{-1}x_j^{-1}.$$

一方面因为 N_i 是正规子群，所以

$$x_i \in N_i, \quad x_j x_i^{-1} x_j^{-1} \in N_i,$$

从而 $x_i x_j x_i^{-1} x_j^{-1} \in N_i$. 另一方面，同样可以知道 $x_i x_j x_i^{-1} x_j^{-1} \in N_j$, 即

$$x_i x_j x_i^{-1} x_j^{-1} \in N_i \cap N_j = \{e\}.$$

这就是说 $x_i x_j x_i^{-1} x_j^{-1} = e$, 即 $x_i x_j = x_j x_i$. 因之，对于任意的 $x, y \in G$, 由

$$x = x_1 \cdots x_s, \quad y = y_1 \cdots y_s$$

有

$$xy = (x_1 y_1) \cdots (x_s y_s).$$

这就证明了上面定义的映射保持乘法，因而是一个同构. □

在这个情形，我们也就说*群 G 分解成正规子群 $N_1, \cdots, N_s$ 的直和*，也称 G *等于 $N_1, \cdots, N_s$ 的* **内直和**.

与线性空间分解成子空间的直和的情况类似，读者不难证明定理 19 中的条件 2) 可以换成

2′) 单位元素只有唯一的表示，即

$$e = e \cdots e;$$

也可以换成

2″) $N_i \cap N_1 \cdots N_{i-1} N_{i+1} \cdots N_s = \{e\}$, $i = 1, \cdots, s$.

正如前面指出的，在群 G 分解成一些正规子群 $N_1, \cdots, N_s$ 的直和时，群 G 的研究也就归结为正规子群 $N_1, \cdots, N_s$ 的研究.

如果一个群不能分解成两个非平凡的正规子群的直和，那么这个群就称为**不可分解的**. 显然，任意一个有限群总可以分解成一些不可分解的群的直和. 群的直和分解是群论中一个重要的问题，这里不细说了.

最后作为一个例子，我们来看看有限交换群的情形.

设 G 是一有限交换群，$|G| = n$, n 的标准分解式为

$$n = p_1^{r_1} \cdots p_s^{r_s},$$

其中 $p_1, \cdots, p_s$ 为不同的素数，$r_i > 0, i = 1, \cdots, s$.

令 G_i 为 G 的西罗 p_i- 子群，$i = 1, \cdots, s$. 由上一节定理 17 推论，可知 G_i 是唯一的西罗 p_i- 子群，因而不难看出 (定理 17)G_i 恰由 G 中全部阶为 p_i 的方幂的元素所组成.

令 $H = G_1 \cdots G_s$. 因为 G_i 中的元素的阶为 p_i 的方幂，而子群

$$G_1 \cdots G_{i-1} G_{i+1} \cdots G_s$$

中元素的阶为 $p_1^{r_1} \cdots p_{i-1}^{r_{i-1}} p_{i+1}^{r_{i+1}} \cdots p_s^{r_s}$ 的因子 (由 §2 定理 6 前的引理), 所以,

$$G_i \cap G_1 \cdots G_{i-1} G_{i+1} \cdots G_s = \{e\}, \quad i = 1, \cdots, s.$$

由定理 19 及上面的讨论可知

$$H \cong G_1 \oplus \cdots \oplus G_s,$$

因之, $|H| = p_1^{r_1} \cdots p_s^{r_s} = |G|$. 这就说明了

$$H = G, \quad G \cong G_1 \oplus \cdots \oplus G_s.$$

换句话说, 我们证明了, *任意一个有限的交换群都可以分解成一些 p- 群的直和*. 当然, 有时交换 p- 群还可分解, 以后我们将证明, 一个 p- 群不可分解的充分必要条件是它是循环群.

§9 若尔当 - 赫德尔定理

在 §4 中我们应用递降子群列刻画了有限可解群. 在这一节我们将指出, 递降子群列对于刻画一般有限群的结构也是一重要的工具, 下面将证明的若尔当 - 赫德尔 (Jordan-Hölder) 定理正说明了这一点.

定义 5 如果一个群 G 的任一个有限递降子群列

$$G = G_0 > G_1 > \cdots > G_r = \{e\} \tag{1}$$

满足: 每个 G_i 是其前一个 G_{i-1} 的正规子群, 则 (1) 称为 G 的一个 **次正规子群列**.(1) 的商群组

$$G_0/G_1, G_1/G_2, \cdots, G_{r-1}/G_r \cong G_{r-1} \tag{2}$$

称为 (1) 的 **因子群组**.

如果一个次正规子群列 (1) 的每个因子群 G_{i-1}/G_i 都是单群, 则 (1) 称为一个 **合成群列**.

在上述定义中 "次" 的意义是并不要求每个子群 G_i 为 G 的正规子群.

在 (1) 中可能有重复的项出现, 也就是在 (2) 中可能有单位元群即 $\{e\}$ 出现. (2) 中非单位元的因子群的个数称为 (1) 的 **长度**.

单群 G 显然只有一个次正规子群列 $G > \{e\}$，它也是唯一的合成群列. 如果 G 不是单群，则它至少有两个次正规子群列. 但是一般的群则不一定有合成群列.

我们首先指出，每个有限群 G 至少有一个合成群列. 设 (1) 是 G 的一个无重复的次正规子群列. (1) 的长度 r 显然不超过 G 的阶. 因此不妨设 (1) 是 G 的一个无重复的具有最大长度的次正规子群列. 我们用反证法来证明它是一个合成群列. 假若有某个因子群 $G_i/G_{i+1} = \overline{G_i}$ 不是单群. 于是 $\overline{G_i}$ 有一个非平凡的正规子群 $\overline{H}$. 根据 §1 群同态定理，在 G_i 与 G_{i+1} 之间存在一个子群 H 使得

$$G_i \rhd H \rhd G_{i+1},$$

而且

$$H/G_{i+1} \cong \overline{H},$$

然后在 (1) 中插入一项 H 使得

$$G = G_0 > \cdots > G_i > H > G_{i+1} > \cdots > G_r = \{e\},$$

这是 G 的一个无重复的次正规子群列. 但是它的长度等于 $r+1$. 这与 (1) 为最大长度的假设矛盾. 所以每个因子群 G_i/G_{i+1} 是单群，从而 (1) 是一个合成群列.

我们实际上是证明了，只要某一因子群 G_i/G_{i+1} 不是单群，那么在 G_i 与 G_{i+1} 之间就可以插入一个子群 H 使次正规子群列的长度增加. 因此，合成群列也就是不能再插入 (真正地) 任何一项的次正规子群列.

证明是严重地依赖于群的有限性. 至于无限群，一般地就不一定有合成群列，如整数加法群 $\mathbf{Z}$(读者验证一下). 为了保证合成群列的存在，对无限群必须加适当的 "有限" 条件，这在本书中就不讨论了.

在 §4 中我们已经得到如下的结论：

1) 每个有限可解群 G 有一个合成群列

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{e\},$$

使得每个因子群 G_i/G_{i+1} 都是素数阶循环群. 反之也成立.

2) 有限可解群 G 的任一个合成群列 (无重复项)$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{e\}$ 的因子群组

$$G_0/G_1, G_1/G_2, \cdots, G_{r-1}/G_r$$

不计次序由 G 本身唯一决定，与合成群列的选取无关.

第一条是有限可解群类的特性，用它可以判别一个有限群是不是可解的．而第二条则不仅是有限可解群所独有的，它是一般有限群类的共性．这表现在

若尔当 - 赫德尔定理 有限群 G 的任意两个无重复项的合成群列有相同的长度，而且它们的因子群组在同构意义下不计次序一一相等．

证明 设

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{e\} \tag{3}$$

和

$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_s = \{e\} \tag{4}$$

是 G 的两个无重复项的合成群列．求证 $r = s$ 而且它们的因子群组

$$G/G_1, \cdots, G_{r-1}/G_r \tag{5}$$

和

$$G/H_1, \cdots, H_{s-1}/H_s \tag{6}$$

在同构意义下不计次序一一相等．证明是对合成群列的长度作归纳法．若 $r = 1$，则 G 为单群．而单群只有一个合成群列，从而 (3),(4) 相同，$r = s = 1$．假设定理对于有一个长度 $r-1$ 的合成群列的有限群成立，求证对于有一个长度 r 的合成群列的有限群定理也成立．

若 $G_1 = H_1$，则在 (3),(4) 中去掉第一项之后，它们就是同一个群 $G_1 = H_1$ 的合成群列，而且它们的长度分别为 $r-1$ 和 $s-1$．根据归纳法假设得 $r-1 = s-1$，从而 $r = s$，而且在 (5),(6) 中去掉头一项之后的因子群组不计次序一一相等，因而 (5),(6) 也一一相等．其次考虑一般情况，设 $G_1 \neq H_1$．我们利用 §1 群同态定理，将一般情况归结为上面的情况，从而证明本定理．由于 G/G_1 和 G/H_1 都是非平凡单群，因而 G_1 和 H_1 都是 G 的极大正规子群．

又因 $G_1 \neq H_1$，可知 $G_1 \cdot H_1 \supset G_1, H_1$，但 $G_1 \cdot H_1 \neq G_1, H_1$．从而

$$G = G_1 \cdot H_1.$$

令 $G_1 \cap H_1 = N_2$．根据 §1 同态定理有

$$G/G_1 \cong H_1/N_2,\quad G/H_1 \cong G_1/N_2. \tag{7}$$

任意取定 N_2 的一个无重复的合成群列 $N_2 \rhd N_3 \rhd \cdots \rhd N_t = \{e\}$，用它作出 G 的两个新的无重复的合成群列

$$G = G_0 \rhd G_1 \rhd N_2 \rhd \cdots \rhd N_t = \{e\} \tag{8}$$

和

$$G = H_0 \rhd H_1 \rhd N_2 \rhd \cdots \rhd N_t = \{e\}. \tag{9}$$

然后比较 (3) 和 (8), 由于第二项相同，于是可归结为上面的情况，从而 $r = t$, 因而因子群组

$$G/G_1, G_1/N_2, N_2/N_3, \cdots, N_{t-1}/N_t \tag{10}$$

和 (5) 不计次序一一相等. 再比较 (4) 和 (9), 第二项也相同, 于是又归结为上面的情况. 从而 $s = t = r$ 而且因子群组

$$G/H_1, H_1/N_2, N_2/N_3, \cdots, N_{t-1}/N_t \tag{11}$$

和 (6) 不计次序一一相等. 由 (7) 可知, (10) 和 (11) 不计次序一一相等, 所以因子群组 (5) 和 (6) 不计次序也一一相等. 这就证明了, 定理对于有一个长度 r 的合成群列的有限群也成立. 由归纳法可知, 定理对任意有限群成立. □

若尔当 - 赫德尔定理告诉我们, 一个有限群 G 的任一合成群列的因子群组 (不计次序) 在同构意义下是由 G 唯一决定的, 与合成群列的选取无关, 因而这个因子群组也称为群 G 的因子群组, 它由一组非平凡的单群组成. 人们自然要提出它的反问题, 就是预先给定一组有限单群 $S = \{S_1, \cdots, S_r\}$, 问以 S 为因子群组的有限群有多少种不同构的类型? 当 $r = 1$ 时, 显然只有一种, 就是 $G \cong S_1$. 当 $r \geq 2$ 时, 这个问题就变得非常困难. 一般说来, 它可以归结为如下的问题: 任意给定两个群 H 和 N, 试构造出所有不同构的群 G 使得 N 为 G 的正规子群而且商群

$$G/H \cong H.$$

这就是所谓的群扩张问题. 群扩张是群论中的一个重要的理论, 它超出本书讨论的范围.

§10 幺半群

现在我们来介绍一个比群更广一点的概念, 即幺半群. 它虽然内容没有群那样丰富, 能得到的结果也不像群那样深刻, 但是它确实概括了不少重要的对象, 在理论与实际中有不少应用. 因之建立这个概念并讨论它的一些基本性质是有必要的.

定义 6 设 S 是一非空集合. 如果在 S 上定义了一个二元运算, 记为 ab (读作乘法), 它适合条件:

1) $a(bc) = (ab)c$ (结合律), $a, b, c \in S$,

2) 在 S 中有一元素 e 具有性质

$$ea = ae = a, \text{ 对所有的 } a \in S;$$

那么 S 就称为一 **幺半群**.

当然，如果把二元运算记为 $a+b$, 那么就读成加法，这是无关紧要的. 显然，所有的群都是幺半群. 下面来看几个例子.

例 1 设 R 是一个幺环. 于是 R 的元素对于乘法就成一个幺半群.

例 2 全体非负整数对于加法成一幺半群；全体正整数对于乘法成一幺半群.

例 3 设 X 是任意一个非空集， $M(X)$ 是 X 的全体到自身的映射组成的集合. $M(X)$ 对于映射的乘法显然成一幺半群.

例 4 设 X 是任意一个非空集合， $P(X)$ 是 X 的全部子集合组成的集合. $P(X)$ 对于集合并 "$\cup$" 成一幺半群； $P(X)$ 对于集合交 "$\cap$" 也成一幺半群.

例 5 设 G 是一个群. 在 G 外任取一个元素 0, 定义 $0g = g0 = 0$, 对所有的 $g \in G$. 于是 $G \cup \{0\}$ 成一幺半群.

在幺半群中，容易证明，适合条件 2) 的元素是唯一的，这个元素称为**单位元素**.

如果幺半群 S 的运算进一步适合交换律，即 $ab = ba$, 那么 S 就称为交换幺半群. 例 2 与例 4 中的幺半群就是交换的.

如果 Q 是幺半群 S 的一个子集合，具有性质： 1) $e \in Q$, 2) Q 对运算封闭，那么 Q 就称为 S 的一个 **子幺半群**. 幺半群 $M(X)$ 的子幺半群称为集合 X 上的一个 **变换幺半群**.

如果 φ 是幺半群 S 到幺半群 S' 的一个映射，它适合条件： 1) $\varphi(e) = e'$ (S' 中的单位元素)， 2) $\varphi(ab) = \varphi(a)\varphi(b)$, 那么 φ 就称为 S 到 S' 的一个 **同态**. 单一的，映上的同态称为 **同构**.

与群的情况一样，可以证明

定理 20 任意一个幺半群 S 都与集合 S 的一个变换幺半群同构.

证明留给读者. □

设 $\varphi : S \to S'$ 是幺半群的同态. 容易证明， φ 的象 $\varphi(S)$ 是 S' 的子幺半群. φ 的核

$$\ker(\varphi) = \{a \in S \mid \varphi(a) = e'\}$$

是 S 的子幺半群.

与群的情形不同，我们不容易刻画出什么样的子幺半群可以是一个同态的核. 因而，为了弄清楚幺半群的同态，我们需要采用另外的办法.

定义 7 设 S 是一幺半群，“$\sim$”是定义在 S 上的一个等价关系．如果“$\sim$”具有性质：由 $a\sim b, c\sim d$ 可以推知 $ac\sim bd$，那么“$\sim$”称为 S 的一个 **同余关系**.

我们知道，全体非负整数对于加法成一幺半群．取一正整数 m，定义

$$a\equiv b \pmod m, \text{ 如果 } m|(a-b).$$

显然这是一个同余关系．我们以前讨论过，在这个同余关系下，全体非负整数被分成 m 个剩余类.

对于一般的幺半群，因为同余关系是一等价关系，所以可以分成若干等价类，在这里称为同余类．设 A,B 是任意两个同余类， $a\in A, b\in B$．由定义可知， ab 所在的同余类与 a,b 的选择无关，而是由 A,B 决定的．我们把 ab 所在的同余类定义为同余类 A 、 B 的乘积，记为 AB．对于这样定义的乘法，结合律是明显的．如果 E 是单位元素 e 所在的同余类，那么显然有

$$AE=EA=A, \text{ 对所有的同余类 } A.$$

定义 8 设 S 是一幺半群， $\sim$ 是定义在 S 上的一个同余关系．全体同余类在上面定义的运算下所成的幺半群称为 S 对于同余关系 $\sim$ 的 **商幺半群**，记为 $S/\sim$.

把幺半群的每个元素映到它所在的同余类．这显然是幺半群到商幺半群的一个同态，这个同态通常称为自然同态．自然同态是满的．这个事实说明，每个同余关系都决定一个同态，反过来我们有

定理 21 *设 $\varphi: S\to S'$ 是幺半群 S 到 S' 的一个同态．在 S 上定义：*

$$a\sim b \text{ 当且仅当 } \varphi(a)=\varphi(b).$$

$\sim$ 是一个同余关系.

证明留给读者. □

以上讨论表明，幺半群上的同余关系与同态有紧密的联系．单位元素所在的同余类就是自然同态的核，它是一个子幺半群.

定理 22 *设 $\sim$ 是定义在幺半群 S 上的一个同余关系， $\pi: S\to S/\sim$ 是自然同态，而 $\varphi: S\to S'$ 是幺半群 S 到 S' 的一个同态．如果当 $a\sim b$ 时必有 $\varphi(a)=\varphi(b)$，那么存在唯一的同态 $\psi: S/\sim\to S'$ 使*

$$\psi\pi=\varphi.$$

证明 设 A 是任意一个同余类. 由定理的条件可知, 在同态 φ 下, A 的元素有相同的象. 我们定义

$$\psi(A)=\varphi(a), \text{ 其中 } a\in A.$$

显然, ψ 是一个同态, 而且 $\psi\pi=\varphi$, 且因 π 是满同态, 所以适合这个条件的 ψ 是唯一的. □

最后我们指出, 如果在幺半群的定义中不要求有单位元素, 换句话说, 对运算只要求结合律, 那么这样的代数结构通常称为 **半群**, 对此我们不打算作过多的讨论.

§11 自由幺半群与自由群

作为本章的结束, 我们来介绍一下自由幺半群与自由群这两个概念. 它们不但在群论中, 而且在其它的数学分支中都有重要的应用.

设 X 是一非空集合, 为了说起来简单一些, 我们总限制 X 是有限集合, 读者不难看出, 所有的讨论都很容易推广到任意集合的情形. 为了确定起见, 设

$$X=\{a_1,a_2,\cdots,a_n\}.$$

任意一个有限长的序列

$$x_1x_2\cdots x_i, \text{ 其中 } x_1,x_2,\cdots,x_i\in X,$$

称为一个 **字**. 如 $a_1a_2a_1a_3, a_1a_1a_3a_1a_2$ 等都是字. 在序列中我们允许长度为零的情形. 就是所谓空字, 记为 Λ. 由集合 X 中的元素组成的字的全体记为 $\widetilde{X}$. 在 $\widetilde{X}$ 上, 把两个字的串连定义为乘法, 即

$$(x_1\cdots x_i)(y_1\cdots y_j)=x_1\cdots x_iy_1\cdots y_j.$$

结合律是明显的, 而空字就是单位元素. $\widetilde{X}$ 在这个运算下成一幺半群.

幺半群 $\widetilde{X}$ 称为由集合 X 生成的 **自由幺半群**.

自由幺半群的一个重要性质是

定理 23 设 X 是一有限非空集合, S 是一个幺半群. 对于任意一个映射 $f:X\to S$ 都存在唯一的同态 $\varphi:\widetilde{X}\to S$ 使

$$\varphi(x)=f(x), \text{ 对所有的 } x\in X.$$

证明 定义 $\varphi:\widetilde{X}\to S$ 为:

$$\varphi(\Lambda)=e,\ e \text{ 为 } S \text{ 的单位元素},$$
$$\varphi(x_1\cdots x_i)=f(x_1)\cdots f(x_i).$$

这就是所要的同态. 唯一性是显然的. □

为什么 $\widetilde{X}$ 中的元素要叫做字呢？假如集合 X 是由 26 个拉丁字母组成的集合，那么任意一个英文字都是 $\widetilde{X}$ 中的一个元素. 这就是字这个名称的由来. 假如 X 中除 26 个字母外，再添进一个符号来表示字与字之间的空格. 譬如说，"*", 那么英文中的一个句子也可以看作这个扩大了的集合上的字. 基于这个来源，集合 X 有时称为字母表. 当然，对于任何一种语言，不论形式的还是自然的，给了一个字母表 X, 并不是 $\widetilde{X}$ 中每个元素都是语言中有意义的字. 有意义的字不过是 $\widetilde{X}$ 的一个子集合. 尽管如此，自由幺半群仍然是研究语言的形式结构的很好的工具.

在自由幺半群的基础上，我们来定义自由群. 仍然令 X 为一有限非空集合，

$$X=\{a_1,\cdots,a_n\},\quad n\geq 1.$$

我们引入一个与 X 一一对应但与 X 无公共元素的集合.

$$X'=\{a_1',\cdots,a_n'\},$$

作它们的并集

$$X^*=X\cup X',$$

考虑由 X^* 生成的自由幺半群 $\widetilde{X}^*$.

$\widetilde{X}^*$ 中两个字 w_1,w_2 称为相邻，如果有 $g,h\in\widetilde{X}^*, a_i\in X$, 使 w_1 与 w_2 中有一个是 $ga_ia_i'h$, 而另一个是 gh, 或者一个是 $ga_i'a_ih$, 而另一个是 gh.

$\widetilde{X}^*$ 中两个字 w_1,w_2 称为等价的，记为

$$w_1\sim w_2,$$

如果在 $\widetilde{X}^*$ 中有一串字 $v_1,v_2,\cdots,v_l$ 适合条件:

1) v_j 与 v_{j+1} 相邻， $j=1,\cdots,l-1$;

2) $v_1=w_1, v_l=w_2$.

容易证明，"$w_1\sim w_2$" 是一等价关系，而且是一同余关系 (读者仔细验证一下). 作商幺半群 $\widetilde{X}^*/\sim$. $\widetilde{X}^*/\sim$ 实际上是一个群. 为了证明 $\widetilde{X}^*/\sim$ 是一个

群，只要证明其中的每个元素都有逆．设 $A\in\widetilde{X^*}/\sim$，而 $x_1x_2\cdots x_l\in A$．对于每个 $x\in X^*$，我们规定

$$x'=\begin{cases}a_j', & 如果\ x=a_j,\\ a_j, & 如果\ x=a_j'.\end{cases}$$

于是在 $\widetilde{X^*}/\sim$ 中取包含字

$$x_l'x_{l-1}'\cdots x_1'$$

的同余类 B．显然

$$x_1\cdots x_lx_l'\cdots x_1'\sim\Lambda,$$

因之在 $\widetilde{X^*}/\sim$ 中， $B=A^{-1}$．

定义 9 群 $\widetilde{X^*}/\sim$ 称为由集合 X 生成的 **自由群**，记为 $F(X)$．

X^* 中的字 w 称为 **可约的**，如果有 $g,h\in\widetilde{X^*},a_i\in X$ 使

$$w=ga_ia_i'h\ 或\ w=ga_i'a_ih,$$

否则称为 **不可约的**．

容易证明，在每一同余类中一定存在一个不可约的字 (对字的长度作归纳法)．事实上，我们还可以证明， 每个同余类中，不可约字是唯一的．这个结论直观上是明显的，可是证明起来却不是一两句话能说清楚的．因之在这里就不谈了．这就是说， $F(X)$ 中的元素全可以用不可约的字来代表，这个表示是唯一的．在 $F(X)$ 中，显然有

$$a_i'=a_i^{-1},\ \ i=1,\cdots,n.$$

当 X 含有一个元素，即 $X=\{a\}$ 时， $F(X)$ 就是前面谈到过的无限循环群．

自由群的一个重要性质是，

定理 24 设 X 是一非空有限集合， G 是一个群．对于任意一个映射 $f:X\to G$ 都存在唯一的同态 $\psi:F(X)\to G$ 使

$$\psi(x)=f(x),\ \ 对所有的\ x\in X.$$

证明 令 $X=\{a_1,\cdots,a_n\}$，对于集合 X^* 的元素，我们定义：

$$f(a_i')=f(a_i)^{-1},\ \ i=1,\cdots,n.$$

于是我们得到一个映射 $f:X^*\to G$．由定理 23，存在一个同态 $\varphi:\widetilde{X^*}\to G$．由 f 的定义可知，如果 $w_1\sim w_2$，那么 $\varphi(w_1)=\varphi(w_2)$．再根据上一节的定理 22，存在一个同态

$$\psi:F(X)=\widetilde{X^*}/\sim\to G.$$

这就是我们所要的同态. 因为 $F(X)$ 是由元素 $a_1,\cdots,a_n$(看作 $F(X)$ 的元素) 生成的, $\psi(a_i)=f(a_i)$, $i=1,\cdots,n$, 所以, ψ 在 $F(X)$ 上的作用是唯一决定的. □

推论 任何一个有限生成的群都同构于一自由群的商群.

证明 设 G 是一有限生成的群, $g_1,\cdots,g_n$ 是 G 的一组生成元. 取一个含 n 个元素的集合,

$$X=\{a_1,\cdots,a_n\}.$$

定义 $f:X\to G$ 为

$$f(a_i)=g_i,\quad i=1,\cdots,n.$$

由定理 24, 有一个同态

$$\psi:F(X)\to G$$

使

$$\psi(a_i)=g_i,\quad i=1,\cdots,n.$$

ψ 显然是一满同态. 令 $\ker(\psi)=N$, 于是由同态基本定理

$$G\cong F(X)/N.\quad □$$

正规子群 N 对于群 G 的意义是什么呢? N 中的元素都可以用符号 $a_1,\cdots,a_n$ 及它们的逆 $a_1^{-1},\cdots,a_n^{-1}$ 组成的不可约字来表示, 字 w 属于 N 就说明, 把 $g_1,\cdots,g_n$ 分别代替 $a_1,\cdots,a_n$, 它在 G 中就等于单位元素 e. 因而

$$w=e$$

实际上是刻画 G 的生成元 $g_1,\cdots,g_n$ 之间的一个关系. 因而, 正规子群 N 表示了 G 的生成元之间的一切关系.

在任意一个群 G 中, 取一子集合 $A\subset G$, 因为任意多个包含 A 的正规子群的交还是一个包含 A 的正规子群, 所以一定存在一个最小的包含 A 的正规子群 (即所有的包含 A 的正规子群之交)N. 这个正规子群 N 称为由 A 所生成的 (注意与 A 生成的子群的差别). 如果一个正规子群 N 可以被一个有限集合生成, 那么 N 就称为有限生成的, 而这个有限集合的元素就称为一组生成元.

我们知道任意一个有限生成的群 G 都同构于一个自由群的商群, 即

$$G\cong F(X)/N,$$

如果 N 在 $F(X)$ 中是有限生成的, 那么我们就说群 G 是**可以有限表现的**. 在这个情况, 设 $w_1,\cdots,w_k$ 是 N 的一组生成元, 于是

$$w_1=e,\cdots,w_k=e$$

就称为群 G 的生成元 $a_1,\cdots,a_n$ 的一组**生成关系**.

以前我们说过，二面体群 D_n 由 a,b 两个元素生成，其中

$$a^n=1,\ \ b^2=1,\ \ b^{-1}ab=a^{-1}.$$

这三个式子就是现在所谓的生成关系. 换成现在语言，取 $X=\{a,b\}$, 于是

$$D_n\cong F(X)/N,$$

其中 N 是由 $a^n,b^2,b^{-1}aba$ 生成的正规子群.

习 题

1. 设 G 为一有限群，$N\lhd G$, $|N|$ 与 $|G/N|$ 互素. 如果元素 a 的阶整除 $|N|$, 则 $a\in N$.

2. 设 c 为群 G 中一个阶为 rs 的元素，其中 $(r,s)=1$, 证明 c 可以表示成 $c=ab$, 其中 a 的阶为 r, b 的阶为 s, 且 a,b 都是 c 的方幂.

3. 如果群 G 中元素 a 的阶与正整数 k 互素，则方程 $x^k=a$ 在 $\langle a\rangle$ 内恰有一解.

4. 证明在一群中，元素 ab 与 ba 有相同的阶.

5. 设 $n>2$. 证明有限群 G 中阶为 n 的元素的个数是偶数.

6. 当 $n>2$ 时，证明 $Z(S_n)=\{e\}$.

7. 证明有理数加法群 $\mathbf{Q}_+$ 的任一有限生成的子群是循环群.

8. 设 G 是一个有限生成的交换群. 如果 G 的每个生成元是有限阶元素，则 G 是有限群.

*9. 设 G 为一群，k 代表正整数. 令 $G^k=\{a^k\,|\,a\in G\}$. 证明 G 是一循环群的充分必要条件是 G 的每个子群都是 G^k 这样的集合.

10. 证明 S_n 由 $n-1$ 个对换 $(12),(13),\cdots,(1n)$ 生成，S_n 也可由 $n-1$ 个对换 $(12),(23),\cdots,(n-1\ n)$ 生成.

11. 证明 S_n 由 (12) 与 $(12\cdots n)$ 生成.

12. 当 $n>2$, 证明 A_n 由 (123) 与 $(12\cdots n)$ 生成 (在 n 为奇数的情形),A_n 由 (123) 与 $(23\cdots n)$ 生成 (在 n 为偶数的情形).

13. 设 $\sigma=(12\cdots n)$, 证明 σ 在 S_n 内的中心化子是 $\langle\sigma\rangle$, 并证明 σ 在 S_n 中的共轭类包含 $(n-1)!$ 个元素.

14. 在 S_5 中确定每个共轭类的一个代表及每个共轭类包含元素的个数，由此证明 S_5 只有三个正规子群，即 $\{e\},A_5,S_5$.

15. 设 H_1,H_2 是群 G 的子群，且它们的交包含 G 的一个正规子群 N. 证明在 G/N 内有

$$H_1/N\cap H_2/N\cong(H_1\cap H_2)/N.$$

16. 设 H_1,H_2 是群 G 的两个子群，证明 $H_1\cap H_2$ 的任一左陪集是 H_1 的一个左陪集与 H_2 的一个左陪集的交.

17. 设 H 是 G 的一个子群，H 在 G 中全体左 (右) 陪集的个数称为 H 在 G 中的**指数**, 记为

$$[G:H].$$

证明，如果子群 H_1, H_2 在 G 中的指数都有限，则 $H_1 \cap H_2$ 的指数也有限.

18. 设 G 为一有限群，$H < G$, 且 $[G:H] = n > 1$. 证明 G 必含有一指数整除 $n!$ 的非平凡正规子群或者 G 同构于 S_n 的一个子群.

19. 设 G 为一有限群，p 为 $|G|$ 的最小素因子. 证明指数为 p 的子群 (如存在) 必正规.

20. 证明 p^2 阶的群 (p 为素数) 必交换，这样的群只有两种不同构的类型.

21. 证明任一非交换的 6 阶群同构于 S_3.

22. 定出全部互不同构的 15 阶群.

23. 定出全部互不同构的 10 阶群.

24. 设 p, q 为不同的素数，证明不存在阶为 pq 的单群.

25. 设 p, q 为不同的素数，证明 p^2q 阶群必包含一个正规的西罗子群.

26. 举出两个有限的非交换群 G, 分别适合

(i) $a^3 = e$, 对所有的 $a \in G$;

(ii) $a^4 = e$, 对所有的 $a \in G$.

27. 设 $H, K < G, a \in G$, 子集合 HaK 称为子群 H, K 的一个**双陪集**. 证明

$$|HaK| = |H|[K : a^{-1}Ha \cap K].$$

28. 如果有限群 G 有一个非平凡的循环的西罗 2- 子群, 则 G 有一个指数为 2 的子群.
(提示：在 G 的正则表示下，循环西罗 2- 子群的生成元对应于 G 上的奇置换.)

29. 设 G 为有限群，A, B 是 G 的两个非空子集合, 如果 $|A| + |B| > |G|$, 则 $AB = G$.

30. 设 H 是有限群 G 的一个非平凡的子群，证明

$$G \neq \cup gHg^{-1}, \quad g \in G.$$

31. 决定 S_4 的西罗 2- 子群和西罗 3- 子群.

32. 证明不存在阶为 56 或 148 的单群.

33. 设 G 为一有限群，$N \lhd G$, P 为 N 的一个西罗子群，T 为 P 在 G 中的正规化子. 证明 $G = NT$.

34. 设 G 为一有限群，P 为 G 的一个西罗 p- 子群，$N \lhd G$. 证明 $P \cap N$ 是 N 的一个西罗 p- 子群，同时 PN/N 是 G/N 的一个西罗 p- 子群.

35. 设 G 为一有限群，$H < G$, P 是 G 的一个西罗 p- 子群. 证明有元素 $a \in G$ 使 $aPa^{-1} \cap H$ 是 H 的一个西罗 p- 子群.

36. 设 p 为一素数，$\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, $G = GL_n(\mathbf{F}_p)$. 具体写出 G 的一个西罗 p 子群，算出它的阶并算出 G 的全部西罗 p- 子群的个数.

37. 设群 G 的阶是 p^3, p 为一素数. 证明, 若 G 非交换, 则

$$G^{(1)} = Z(G).$$

38. 设 G 为一 p- 群, 即 $|G| = p^n, N \lhd G, |N| = p$. 证明

$$N < Z(G).$$

39. 如果 $G/Z(G)$ 是循环群, 则 G 交换.

40. 证明任一有限群都同构于 A_n 的一个子群, n 为一适当的正整数.

41. 设 G 为一群, $N \lhd G, N \cap G^{(1)} = \{e\}$. 证明 $N < Z(G)$.

42. 证明可解群的子群、商群都是可解群.

43. 证明阶为 p^2q 的群必可解, 其中 p, q 是不同的素数.

44. 证明 p- 群一定是可解群.

45. 设 H, K 是群 G 的正规子群. 如果 G/H 与 G/K 都可解, 则 $G/H \cap K$ 也可解.

46. 如果群 G 恰有两个自同构, 则 G 必交换.

47. 证明阶 > 2 的有限群至少有两个自同构.

48. 证明四元群 $V = \{e, (12)(34), (13)(24), (14)(23)\}$ 的自同构群与 S_3 同构.

49. 证明 S_3 与 S_4 都是完全群.

50. 设 G 为一非交换的单群, 证明 $\mathrm{Aut}(G)$ 是一完全群.

*51. 证明不存在群 G 适合条件

$$G > S_4 \text{ 且 } G^{(1)} = S_4.$$

52. 证明: 在交错群 A_n, $n > 4$ 中每个 3- 轮换都可以表示成一换位子. 由此证明 $A_n^{(1)} = A_n$.

53. 证明 S_4 由元素 a, b 生成, 而 a, b 适合

$$a^2 = b^3 = e, \quad (ab)^4 = e.$$

54. 证明 A_4 由元素 a, b 生成, 而 a, b 适合

$$a^2 = b^3 = e, \quad (ab)^3 = e.$$

55. 设一个群 G 由元素 a, b 生成, 而 a, b 适合

$$a^4 = b^4 = 1, \quad a^2 = b^2, \quad b^{-1}ab = a^{-1}.$$

证明 G 为一 8 阶群且非交换, 它的全部子群都正规.

证明群 G 与四元数乘法群

$$H = \{\pm 1, \pm I, \pm J, \pm K\}$$

同构.

*56. 证明阶小于 60 的群或者是素数阶的循环群或者是可解群; 而阶为 60 的单群与 A_5 同构.

(提示: 首先决定 60 阶单群 G 的西罗 5- 子群和西罗 3- 子群的个数以及 5 阶元和 3 阶元的个数, 然后根据 2 阶元和 4 阶元的个数决定西罗 2- 子群的个数. 最后用 G 的元素对西罗 2- 子群的集合 $\{Q_2\}$ 作变换 $Q_2 \mapsto aQ_2a^{-1}$, $a \in G$.)

*57. 证明: 若群 G 是有限生成的, 则它的指数有限的子群 H 也是有限生成的.

(提示: 设 G 的生成元为 g_i $(i = 1, \cdots, n)$, G 关于 H 的左陪集代表为 a_j $(j = 1, \cdots, m)$. 则 $a_j^{-1}g_ia_k$ $(i = 1, \cdots, n, j, k = 1, \cdots, m)$ 中属于 H 的元素生成 H.)

第三章　环

第一章已经介绍了环、理想、商环以及环同态等概念并建立了环同态基本定理. 本章进一步给出环的几个重要的同态定理并介绍几种构造环的方法.

§1　环的同态定理

在建立环同态定理之前，先介绍理想的运算. 设 H,N 为环 R 的子环，则**交** $H\cap N$ 为 R 的子环. 因为首先 $H\cap N$ 是 R 的一个加法子群而且对乘法封闭，因而 $H\cap N$ 是一个子环. 如果进一步假设 N 是 R 的理想，则 $H\cap N$ 显然是 H 的理想. 如果 H 和 N 都是 R 的理想，则 $H\cap N$ 也是 R 的理想. 这是因为，若 $a\in H\cap N, r\in R$, 则 $ar, ra\in H$ 且 $ar, ra\in N$, 因而 $ar, ra\in H\cap N$, 所以 $H\cap N$ 为 R 的理想.

环 R 的子环 H 与 N 的 **和**, 如群论一样，定义为

$$H+N=\{a+b\,|\,a\in H, b\in N\}.$$

$H+N$ 是 R 的一个加法子群, 但不一定是 R 的子环. (见下面的例子) 若还假定 N 是 R 的理想, 则 $H+N$ 是 R 的一个子环. 因为，对于 $a_i\in H, b_i\in N, i=1,2$ 有

$$(a_1+b_1)(a_2+b_2)=a_1a_2+a_1b_2+b_1a_2+b_1b_2,$$

其中后三项属于 N 而 $a_1a_2\in H$, 从而上式左端属于 $H+N$. 所以 $H+N$ 是一个子环.

若 H,N 都是 R 的理想, 则 $H+N$ 也是 R 的理想. 因为 $a\in H, b\in N, r\in R$ 有 $r(a+b)=ra+rb\in H+N$. 同样, $(a+b)r\in H+N$. 所以 $H+N$ 是 R 的理想.

例 设 R 为一个数域 F 上 2×2 全矩阵环. 令

$$H=\left\{\begin{pmatrix}0&0\\a&0\end{pmatrix}\,\middle|\,a\in F\right\},$$

$$N=\left\{\begin{pmatrix}0&b\\0&0\end{pmatrix}\,\middle|\,b\in F\right\}.$$

H,N 都是 R 的子环, 但 $H+N$ 不是 R 的子环.

下面是关于环的几个同态定理. 它们和群的同态定理是平行的.

设 $\sigma: R\to R'$ 是一个环同态而且是满的, N 是它的核. σ 诱导出 R 的子环到 R' 的子环的映射. 设 H 为 R 的一个子环, 由群论可知象集 $\sigma(H)$ 是 R' 的

一个加法子群而且对乘法封闭，因而 $\sigma(H)$ 是一个子环. 如果 H 是 R 的理想，则 $\sigma(H)$ 也是 R' 的理想. 因为，对于 $r' \in R', a' \in \sigma(H)$，存在 $r \in R$ 和 $a \in H$ 使得 $\sigma(r) = r', \sigma(a) = a'$. 于是 $r'a' = \sigma(r)\sigma(a) = \sigma(ra) \in \sigma(H)$. 同理 $a'r' \in \sigma(H)$. 所以 $\sigma(H)$ 是 R' 的理想.

反之，σ 又诱导出 R' 的子环到 R 的子环的映射. 设 H' 为 R' 的一个子环，由群论可知， H' 在 σ 下的完全反象 $\sigma^{-1}(H')$ 是 R 的一个加法子群而且对乘法封闭，因而 $\sigma^{-1}(H')$ 是 R 的子环. 而且 $\sigma^{-1}(H')$ 包含核 N. 如果 H' 还是 R' 的理想，则 $\sigma^{-1}(H')$ 也是 R 的理想. 因为对于 $r \in R, a \in \sigma^{-1}(H')$，于是 $\sigma(a) \in H'$，从而 $\sigma(ra) = \sigma(r)\sigma(a) \in H'$，所以 $ra \in \sigma^{-1}(H')$. 同理， $ar \in \sigma^{-1}(H')$. 所以 $\sigma^{-1}(H')$ 是 R 的理想.

由第二章 §1 可知，这两种映射有如下关系

$$\sigma^{-1}(\sigma(H)) = H + N,$$
$$\sigma(\sigma^{-1}(H')) = H'.$$

特别，如果 H 包含 σ 的核 N，则有

$$\sigma^{-1}(\sigma(H)) = H.$$

这就证明了

定理 1 设 $\sigma: R \to R'$ 是一个满的环同态， N 是它的核. 则 σ 诱导出 R 的一切包含 N 的子环集合到 R' 的一切子环集合的一个一一对应 $H \mapsto \sigma(H)$，而且在这个对应下理想和理想对应. □

其次进一步考察在环的满同态 $\sigma: R \to R'$ 下由对应的理想得到的商环之间的关系. 设 H 为任一个包含 $\ker(\sigma) = N$ 的 R 的理想. 令 $\sigma(H) = H'$. 首先根据群同态定理，加法群 R/H 和加法群 R'/H' 同构，而且 $\overline{\sigma}: x + H \to \sigma(x) + H'$ 就是它们的一个同构映射. 我们来证明 $\overline{\sigma}$ 还保持乘法. 因为

$$\begin{aligned}\overline{\sigma}((a+H)\cdot(b+H)) &= \overline{\sigma}(ab+H) = \sigma(ab) + H' \\ &= \sigma(a)\cdot\sigma(b) + H' = (\sigma(a)+H')(\sigma(b)+H') \\ &= \overline{\sigma}(a+H)\cdot\overline{\sigma}(b+H),\end{aligned}$$

所以 $\overline{\sigma}$ 是一个环同构. 于是得到

定理 2 设 $\sigma: R \to R'$ 是一个环的满同态， $N = \ker(\sigma)$. H 为 R 的任一包含 N 的理想. 则 σ 诱导出环同构 $\overline{\sigma}: R/H \to \sigma(R)/\sigma(H)$ 使得

$$\overline{\sigma}(x + H) = \sigma(x) + \sigma(H).$$

若将 R' 与 R/N 等同使得 $\sigma(x)=x+N$, 则得

$$R/H \cong (R/N)/(H/N),$$

而且 $\overline{\sigma}: a+H \mapsto \sigma(a)+\sigma(H)$ 是它们的一个同构映射. □

最后我们来考察在环同态 $\sigma: R \mapsto R'$ 下具有同一个同态象的 R 的一切子环之间的关系. 设 $N=\ker(\sigma)$, 设 H 为 R 的任一子环. 令 $\sigma(H)=H'$. 一方面 σ 诱导出一个满的环同态 $H \mapsto H'$, 它的核显然等于交 $H\cap N$, 因而 $H/H\cap N \cong H'$. 另一方面, 将 H 扩充, 作和 $H+N$, 它还是 R 的一个子环而且 $\sigma(H+N)=\sigma(H)=H'$. σ 诱导出环的满同态 $H+N\to H'$、其核 $=N$. 因而 $H+N/N\cong H'$. 最后得到

定理 3 设 H 为环 R 的一个子环, N 为 R 的一个理想, 于是商环 $H/H\cap N$ 和商环 $H+N/N$ 同构

$$H/H\cap N \cong H+N/N,$$

而且映射 $x+N \mapsto x+(H\cap N)$ 是 $H+N/N$ 到 $H/H\cap N$ 的一个同构映射. □

注 定理 2 是环同态基本定理的一个推广. 在定理 2 中取 $H=N$, 即得环同态基本定理.

例 整数环 $\mathbf{Z}$ 的任一理想 N 首先是 $\mathbf{Z}$ 的一个加法子群, 因而 N 是由一个非负整数 n 的一切倍数 $q\cdot n$, $q\in\mathbf{Z}$, 组成. N 可以记成 (n). 现在来求 $\mathbf{Z}$ 的任意两个理想 $(n),(m)$ 的和与交. $(n)+(m)$ 是由一切整数 $rn+sm$ $(r,s\in\mathbf{Z})$ 组成. 由第零章 §3 定理 2 可知 $(n)+(m)$ 是由 n,m 的最大公因子 d 的一切倍数组成, 即 $(n)+(m)=(d)$. $(n)\cap(m)$ 是由 n,m 的一切公倍数组成, 因而是由 n,m 的最小公倍数 M 的一切倍数组成, 即 $(n)\cap(m)=(M)$. 根据本节定理 3 有

$$(n)+(m)/(m) \cong (n)/(n)\cap(m),$$

即得

$$(d)/(m) \cong (n)/(M).$$

假设 m,n 不全为 0, 不妨设 $n\neq 0$. 可以数一下两边商环的元素的个数, 左边有 $\frac{m}{d}$ 个而右边有 $\frac{M}{n}$ 个. 于是 $\frac{m}{d}=\frac{M}{n}$, 即 $dM=mn$. 这表明, 定理 3 重新导出整数环的一个事实: 两个非负整数 m,n 的积 mn 等于它们的最大公因子 d 和最小公倍数 M 的积.

§2 环的直和

在这一节我们介绍环的直和，它是和群的直和相平行的概念，这一节讨论的环都假定是有单位元素环，即幺环，以后不再一一声明．幺环的非零元素 a 的零次方 a^0 规定为 1.

定义 1 设 $R_1,\cdots,R_r$ 为 r 个环．首先作加法群 $R_1,\cdots,R_r$ 的直和 $R=R_1\oplus\cdots\oplus R_r$，然后在 R 中定义乘法如下

$$(a_1,\cdots,a_r)\cdot(b_1,\cdots,b_r)=(a_1b_1,\cdots,a_rb_r),$$

则 R 成一环，它叫做环 $R_1,\cdots,R_r$ 的 **直和**.

R 满足环的条件，读者自己可以验证． R 的零元素是 $(0,\cdots,0)$．若 R_i 有单位元素 1_i，$i=1,\cdots,r$，则 R 有单位元素 $(1_1,\cdots,1_r)$．如果 $R_1,\cdots,R_r$ 都是交换环，则 R 也是交换环.

直和 $R=R_1\oplus\cdots\oplus R_r$ 有 r 个子环

$$R_i'=\{(0,\cdots,0,a_i,0,\cdots,0)\,|\,a_i\in R_i\},\ i=1,\cdots,r.$$

它们适合

1) 每个 R_i' 是 R 的理想而且 $R_i'\cong R_i$;

2) $R=R_1'+\cdots+R_r'$;

3) $R_i'\cap(R_1'+\cdots+\hat{R}_i'+\cdots+R_r)=(0)$, $i=1,\cdots,r$,

其中 $\hat{R}_i'$ 表示在和中去掉了 R_i', (0) 表示零理想;

4) R 的元素表成 $R_1',\cdots,R_r'$ 的元素的和，其表法是唯一的;

5) 当 $i\neq j$ 时， R_i' 的元素与 R_j' 的元素相乘恒为 0, 记成 $R_i'\cdot R_j'=(0)$.

2) 至 4) 由群的直和知道是成立的． 1) 是显然的．现验证 5)．设 $a\in R_i',b\in R_j'$, 由于 1),$ab\in R_i',ab\in R_j'$, 因而 $ab\in R_i'\cap R_j'$．由 3) 得 $ab=0$.

与群论定理相平行的有

定理 4 设环 R 的子环 $R_1,\cdots,R_r$ 适合

1) 每个 R_i 为 R 的理想;

2) $R=R_1+\cdots+R_r$;

3) $R_i\cap(R_1+\cdots+\hat{R}_i+\cdots+R_r)=(0)$, $i=1,\cdots,r$;

则 R 与环 $R_1,\cdots,R_r$ 的直和同构. □

如果一个环 R 的子环 $R_1,\cdots,R_r$ 满足定理 4 的条件，则称 R 是 $R_1,\cdots,R_r$ 的 **内直和**. 基于定理 4, 在环同构意义下，直和与内直和概念是一件事物的两个方面.

定理 4 有一种对偶的形式．在叙述这种对偶形式之前，先引进几个概念.

设 H 和 N 是环 R 的理想. 由 H 的元素和 N 的元素的积作成的有限和

$$\sum a_ib_i,\ \ a_i \in H,\ b_i \in H.$$

组成的集合显然是 R 的一个理想. 这个理想叫做 H 和 N 的 **积**, 记成 $H \cdot N$. $H \cdot N$ 是一个理想, 请读者自己验证之. 读者还可证明理想的乘法对理想的加法满足分配律: 设 H,N,K 为环 R 的理想. 则有

$$H \cdot (N+K) = H \cdot N + H \cdot K,$$
$$(N+K)H = N \cdot H + K \cdot H.$$

如果幺环 R 的理想 H,N 满足 $H+N=R$, 则 H,N 叫做 **互素**.

引理 *设 H,N,K 为幺环 R 的理想, 则有*

1) 若 R 为交换环, 则从 H,N 互素可推出等式 $H \cdot N = H \cap N$;

2) 若 H 与 K 都和 N 互素, 则 $H \cdot K$ 也与 N 互素.

证明 1) 首先显然有 $H \cdot N \subset H \cap N$. 证明反包含也成立. 设 $c \in H \cap N$. 由假设 $H+N=R$, 存在元素 $a \in H, b \in N$ 使得 $a+b=1$. 用 c 右乘等式两端 $ac+bc=c$. 于是 $ac \in HN$. 由于 R 交换, $bc=cb \in HN$. 因而 $c \in HN$, 即得 $H \cap N \subset HN$. 所以 $H \cdot N = H \cap N$.

2) 由假设 $H+N=R$, $K+N=R$. 于是存在元素 $a \in H, b \in K, c, d \in N$ 使得 $a+c=1, b+d=1$. 等式两边分别相乘得

$$1 = (a+c)(b+d) = ab + (ad+cb+cd).$$

等式右端 ad, cb, cd 都属于 N, 而 $ab \in HK$, 因而 1 属于 $HK+N$. 由于 $HK+N$ 是 R 的理想, 对任意 $x \in R, x = x \cdot 1 \in HK+N$. 所以 $R \subset HK+N$. 反之, 显然 $HK+N \subset R$. 最后得 $HK+N=R$. 这表明 HK 与 N 互素. □

定理 5 *设幺环 R 的理想 $N_1, \cdots, N_r$ 两两互素, 则*

$$R/N_1 \cap \cdots \cap N_r \cong R/N_1 \oplus \cdots \oplus R/N_r.$$

而且令 σ_i 表示自然同态 $R \to R/N_i$, $i=1,\cdots,r$. 则映射

$$\sigma: R \to R/N_1 \oplus \cdots \oplus R/N_r,$$
$$x \mapsto \sigma(x) = (\sigma_1(x), \cdots, \sigma_r(x))$$

是一个满同态而且核 $= N_1 \cap \cdots \cap N_r$.

证明 令 $M_i = N_1 \cdots N_{i-1}N_{i+1} \cdots N_r, i=1,\cdots,r$. 于是 $M_1 + M_2 = (N_2 + N_1)N_3 \cdots N_r = N_3 \cdots N_r$, $M_1 + M_2 + M_3 = (N_3 + N_1N_2)N_4 \cdots N_r$, 根据引理

2), N_3 与 N_1N_2 互素，有 $N_3+N_1N_2=R$, 从而得 $M_1+M_2+M_3=N_4\cdots N_r$. 依此类推最后得 $M_1+\cdots+M_r=R$. 因而存在元素 $e_i\in M_i$, $i=1,\cdots,r$ 使得 $e_1+\cdots+e_r=1$. 于是由于 $M_j\subset N_i$, $i\neq j$, 得

$$\sigma_i(e_j)=0,\quad i\neq j;$$
$$\sigma_i(e_i)=1+N_i,\quad i,j=1,\cdots,r.$$

首先证明 σ 是满的. 任给 R 的 r 个元素 $x_1,\cdots,x_r$. 作 $x=e_1x_1+\cdots+e_rx_r$, 于是

$$\begin{aligned}\sigma_i(x)&=\sigma_i(e_1)\sigma_i(x_1)+\cdots+\sigma_i(e_r)\sigma_i(x_r)\\&=\sigma_i(e_i)\sigma_i(x_i)=\sigma_i(x_i),\end{aligned}$$

$$\sigma(x)=\big(\sigma_1(x),\cdots,\sigma_r(x)\big)=\big(\sigma_1(x_1),\cdots,\sigma_r(x_r)\big),$$

因而 σ 是满的. 其次证明 $\ker(\sigma)=N_1\cap\cdots\cap N_r$. 显然 $N_1\cap\cdots\cap N_r\subset\ker(\sigma)$. 反之，设 $\sigma(x)=0$, 于是 $\sigma_i(x)=0$ 对所有 i. 从而 $x\in N_i$ 对所有 i, 即 $x\in N_1\cap\cdots\cap N_r$. 这就完全证明了定理. □

整数环 $\mathbf{Z}$ 的同余概念可以推广到任意环. 设 N 为 R 的一个理想. 对于任意元素 $a,b\in R$, 若 $a-b\in N$, 则 a,b 叫做**模 N 同余**, 记作

$$a\equiv b\pmod{N}.$$

否则， a,b 叫做**模 N 非同余**, 记作 $a\not\equiv b\pmod{N}$. 关于模理想的同余式具有模整数的同余式的基本性质. R 的元素按模 N 分解成一些同余类，含元素 a 的同余类记作 $\bar a$, $\bar a$ 表示商环 R/N 的一个元素. 一个同余方程

$$ax\equiv b\pmod{N},$$

其中 $a\not\equiv 0\pmod{N}$, $a,b\in R$, 在 R 内是否有解意味着方程 $\bar a\cdot\bar x=\bar b$ 在商环 R/N 内是否有解？于是定理 5 可以用同余方程组的形式表示出来，这就是

定理 6 (中国剩余定理) *设幺环 R 的理想 $N_1,\cdots,N_r$ 两两互素，则对任意给定的 r 个元素 $b_1,\cdots,b_r\in R$, 同余方程组*

$$\begin{cases}x\equiv b_1\pmod{N_1},\\ x\equiv b_2\pmod{N_2},\\ \cdots\cdots\cdots\cdots\cdots\cdots\\ x\equiv b_r\pmod{N_r}\end{cases}$$

在 R 内恒有解. 而且它的解 $\bmod N_1\cap\cdots\cap N_r$ 是唯一的, 即任两解 $\bmod N_1\cap\cdots\cap N_r$ 同余.

证明 根据上面的解释，读者不难将定理 5 翻译成定理 6 的形式. □

说明 定理 5 的一个特殊情况值得提一下，就是

定理 5′ *若幺环 R 的理想 $N_1,\cdots,N_r$ 两两互素而且 $N_1\cap\cdots\cap N_r=(0)$，则*

$$R\cong R/N_1\oplus\cdots\oplus R/N_r.\quad \square$$

这个定理和定理 4 互为对偶. 若幺环 R 的理想 $N_1,\cdots,N_r$ 满足定理 5′ 的条件，则 $R_i=N_1\cap\cdots\cap\hat{N}_i\cap\cdots\cap N_r$，$i=1,\cdots,r$，满足定理 4 的条件而且 $R_i\cong R/N_i$. 因而定理 4 可导出定理 5′. 反之，若 R 的理想 $R_1,\cdots,R_r$ 满足定理 4 的条件，则 $N_i=R_1+\cdots+\hat{R}_i+\cdots+R_r$，$i=1,\cdots,r$，满足定理 5′ 的条件而且 $R/N_i\cong R_i$. 因而定理 5′ 导出定理 4.

例 整数环 $\mathbf{Z}$ 的任一理想 N，若 $N\neq(0),N\neq R$，则 $N=(n)$，$n>1$. 将 n 分解成素因子方幂的积 $n=p_1^{e_1}\cdots p_r^{e_r},e_i\geq 1$. 于是

$$(n)=(p_1^{e_1})(p_2^{e_2})\cdots(p_r^{e_r}).$$

根据本节引理 1)，得

$$(n)=(p_1^{e_1})\cap\cdots\cap(p_r^{e_r}).$$

显然理想 $(p_1^{e_1}),\cdots,(p_r^{e_r})$ 两两互素. 根据定理 5，得

$$\mathbf{Z}/(n)\cong\mathbf{Z}/(p_1^{e_1})\oplus\cdots\oplus\mathbf{Z}/(p_r^{e_r}).$$

在这一节中最后介绍理想的生成元. 设 R 为任一环，S 为 R 的任一非空子集. R 中包含 S 的一切理想的交叫做 **由 S 生成的理想**，记成 (S). 它是包含 S 的最小理想，就是说，若理想 N 包含 S，则 N 也包含 (S). S 叫做 (S) 的 **生成元集**. (S) 可以有不同的生成元集. 若 S 是一个有限集 $\{a_1,\cdots,a_r\}$，则 (S) 叫做 **有限生成** 的，而且 (S) 记作 $(a_1,\cdots,a_r)$. 由一个元生成的理想 (a) 叫做 **主理想**. 不难证明，主理想 (a) 是由下列形状的元素

$$na,xa,ay,xay,$$

其中 $n\in\mathbf{Z},x,y\in R$，的一切有限和组成.

若 R 为交换环，则主理想 (a) 由形如 na,xa $(n\in\mathbf{Z},x\in R)$ 的元素的一切有限和组成. 若 R 为有单位元素 e 的交换环，则 $na=(ne)a,ne\in R$. 因而主理想 (a) 由一切元素 xa $(x\in R)$ 组成. 此时 (a) 也可写成 Ra.

最后显然有 $(a_1,\cdots,a_r)=(a_1)+\cdots+(a_r)$.

§3 环的反同构

环不仅有同构的概念而且有反同构的概念. 反同构概念对一类结合代数的研究具有重要性. 在高等代数中给我们提供了很好的例子.

用 $M_n(F)$ 表示数域 F 上 $n\times n$ 全矩阵环, A^T 表示矩阵 A 的转置. 我们知道 $M_n(F)$ 到自身的转置映射 $A\mapsto A^T$ 满足

$$(A+B)^T=A^T+B^T,$$
$$(A\cdot B)^T=B^T\cdot A^T.$$

这个映射叫做 $M_n(F)$ 的反自同构. 把它引伸到一般环有

定义 2 如果环 R 到环 R' 的一个一一对应 σ 满足

1) $\sigma(a+b)=\sigma(a)+\sigma(b)$,

2) $\sigma(a\cdot b)=\sigma(b)\cdot\sigma(a)$,

则 σ 叫做 R 到 R' 的一个 **反同构**, 而且说 R 和 R' 成反同构. 当 $R'=R$ 时, σ 叫做 R 的 **反自同构**.

若环 R 和环 R' 成反同构而且 R 交换, 则 R' 也交换. 此时反同构也是同构.

除了上述域上全矩阵环 $M_n(F)$ 一类例子外, 下面举出两个类型的例子.

例 1 在第一章已经给出实数域 $\mathbf{R}$ 上四元数体 H. H 由下列元素组成:

$$\alpha=a_1+a_1I+a_2J+a_3K,$$

其中 $a_i\in\mathbf{R}$, $1,I,J,K$ 是 H 对 $\mathbf{R}$ 的一基. 它们的运算规定如下

$$I^2=J^2=K^2=-1,\quad I\cdot J=-J\cdot I=K,$$
$$J\cdot K=-K\cdot J=I,\quad K\cdot I=-I\cdot K=J.$$

H 到自身的映射 $\sigma:\alpha\mapsto\overline{\alpha}=a_0-a_1I-a_2J-a_3K$ 是一个一一对应而且保持加法. σ 还是 H 的一个反自同构. 设 $\beta=b_0+b_1I+b_2J+b_3K\in H$. 由计算可知

$$\overline{\alpha\cdot\beta}=\overline{\beta}\cdot\overline{\alpha}.$$

由基的乘法表也容易知道上式成立. 比如, 上式左端带系数 a_1b_2 的项为 $\overline{(a_1I)\cdot(b_2J)}$, 而上式右端带系数 a_1b_2 的项为 $\overline{b_2J}\cdot\overline{a_1I}$, 它们都等于 $-a_1b_2K$. 所以 $\overline{\alpha\cdot\beta}=\overline{\beta}\cdot\overline{\alpha}$. 所以 σ 是 H 的一个反自同构, 而且有 $\sigma^2=1$.

例 2 四元数体 H 上的 2×2 矩阵

$$A=\begin{pmatrix}\alpha&\beta\\\gamma&\delta\end{pmatrix},\quad \alpha,\beta,\gamma,\delta\in H$$

全体记成 $M_2(H)$. 规定矩阵的加法为对应元素相加，矩阵的乘法规定为

$$A\cdot B=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\cdot\begin{pmatrix}\alpha' & \beta'\\ \gamma' & \delta'\end{pmatrix}=\begin{pmatrix}\alpha\alpha'+\beta\gamma' & \alpha\beta'+\beta\delta'\\ \gamma\alpha'+\delta\gamma' & \gamma\beta'+\delta\delta'\end{pmatrix},$$

(因为 H 不交换， A,B 相乘时，注意 A,B 的元素相乘的先后次序) 用 $\overline{A}$ 表示

$$\overline{A}=\begin{pmatrix}\overline{\alpha} & \overline{\beta}\\ \overline{\gamma} & \overline{\delta}\end{pmatrix}.$$

A^T 表示 A 的转置. 于是显然有 $\overline{A+B}=\overline{A}+\overline{B}$. 不难验证下式成立

$$(\overline{A\cdot B})^T=\overline{B}^T\cdot\overline{A}^T.$$

因此 $M_2(H)$ 到自身的映射 $\sigma: A\mapsto \overline{A}^T$ 是一个反自同构，而且 $\sigma^2=1$. 这显然可以推广到四元数体 H 上 $n\times n$ 全矩阵环 $M_n(H)$.

一个环 R 的自同构和反自同构全体对映射的合成为一群，记作 G. R 的自同构全体 $\mathrm{Aut}(R)$ 为 G 的一个子群. 读者自已证明 $\mathrm{Aut}(R)$ 在 G 内的指数 ≤ 2.

对任一非交换环 R, 恒可作出一个环 R' 使得 R' 与 R 成反同构. 首先作一个集合 $R'=\{x'\,|\,x\in R\}$ 使得 R' 与集合 R 成一一对应 $x\mapsto x'$. 然后规定 R' 的运算如下

$$x'+y'=(x+y)',$$
$$x'\cdot y'=(yx)'.$$

于是 R' 成一环而且与环 R 成反同构.

存在没有反自同构的非交换环. 作为习题，请读者举出这样的例子.

§4 素理想和极大理想

从这一节起讨论的环都假定是有单位元素 1 的交换环即交换的幺环. 这一节讨论两种重要的理想, 即素理想和极大理想. 它们不仅为我们提供了一种构造整环和域的方法，而且是研究交换代数的必要的工具. 设 R 是一个交换幺环, N 为 R 的一个理想. 问 N 在什么条件下使得商环 R/N 为一个域或整环？

定义 3 设 R 为一个交换幺环.

1) 若 R 的一个理想 $P\neq R$, 而且从 $a\cdot b\in P$ 恒有 $a\in P$ 或 $b\in P$, 则 P 叫做 R 的一个 **素理想**.

2) 若 R 的一个理想 $M\neq R$ 而且不再存在理想 A 使得 $M\subsetneqq A\subsetneqq R$, 则 M 叫做 R 的一个 **极大理想**.

例 在整数环 $\mathbf{Z}$ 内由素数 p 生成的理想 (p) 是一个素理想. 因为若 $a\cdot b\in(p)$, 则 $p|a\cdot b$. 于是 $p|a$ 或 $p|b$ 即 $a\in(p)$ 或 $b\in(p)$. 显然 $(p)\neq\mathbf{Z}$. 所以 (p) 是一个素理想. 而且 (p) 还是极大理想. 因为若 $\mathbf{Z}$ 有一个理想 (n) 使得 $(p)\subset(n)\subset\mathbf{Z}$, 由 $(p)\subset(n)$ 可知, $n|p$. 因 p 为素数, $n=1$ 或 p. 若 $n=1$, 则 $(n)=\mathbf{Z}$. 若 $n=p$, 则 $(n)=(p)$. 读者自己可以证明, 除由素数生成的素理想外, 其它非零素理想和极大理想是不存在的.

定理 7 *设 R 为一个交换幺环, 于是*

1) 设 $\sigma: R\to R'$ 是环的满同态, $N=\ker(\sigma)$. 则 σ 诱导出 R 的包含 N 的极大理想和 R' 的极大理想成一一对应.

2) R 为一域的充要条件是零理想 (0) 为极大理想.

3) R 的理想 $M\neq R$ 为极大理想的充要条件是 R/M 为一域.

证明 1) 根据本章 §1 定理 1,σ 诱导出 R 的包含 N 的理想和 R' 的理想之间的一个一一对应, 而且显然保持包含关系, 即 R 的包含 N 的理想 H,K 有 $H\subset K \iff \sigma(H)\subset\sigma(K)$. 因此, R 的包含 N 的极大理想与 R' 的极大理想一一对应.

2) 设 R 为一域. 若 H 为 R 的任一非零理想, 则 H 包含一个非零元 a, 由于 $a^{-1}\in R$, H 也包含 $a^{-1}a=1$. 从而 H 包含 R 的一切元, $H=R$. 所以 (0) 是一个极大理想. 反之, 设 (0) 为极大理想. 设 a 为 R 的任一非零元. 则 $Ra=\{xa\ x\in R\}$ 是 R 的一个理想 (因为 R 交换), 而且 Ra 包含 $1\cdot a=a$, 因而 $Ra\supset(0)$ 但 $Ra\neq(0)$. 由于 (0) 为极大, $Ra=R$, 从而 $1\in Ra$, 于是存在一个元 $b\in R$ 使得 $ba=1$. a 在 R 内可逆, 所以 R 为一域.

3) 若 M 为极大, 根据 1), 则 (0) 为 R/M 的一个极大理想. 根据 2),R/M 为一域. 反之, 若 R/M 为一域, 则 (0) 为 R/M 的极大理想, 因而 M 为 R 的极大理想. □

定理 8 *设 R 为一个交换幺环, 则*

1) R 的理想 $P\neq R$ 为素理想的充要条件是 R/P 为整环;

2) R 为整环的充要条件是 (0) 为素理想;

3) 设 $\sigma: R\to R'$ 为满的环同态 $N=\ker(\sigma)$, 则 σ 诱导出 R 的包含 N 的素理想和 R' 的素理想成一一对应.

证明 1) 设 P 为素理想, 求证 R/P 为整环. 若 R/P 的一对元素 $\bar{a},\bar{b}$ 适合 $\bar{a}\cdot\bar{b}=0$, 于是 $\bar{a}\cdot\bar{b}=\overline{ab}=0$, 从而 $ab\in P$. 因 P 为素理想, 从 $ab\in P$ 得 $a\in P$ 或 $b\in P$ 即 $\bar{a}=0$ 或 $\bar{b}=0$, 所以 R/P 为整环. 反之, 设 R/P 为整环, 求证 P 为素理想. 设 $a\cdot b\in P$, 于是在 R/P 内 $\bar{a}\cdot\bar{b}=0$. 因 R/P 为整环, 于是 $\bar{a}=0$ 或 $\bar{b}=0$, 即 $a\in P$ 或 $b\in P$, 所以 P 为素理想.

2) 在 1) 中令 $P=(0)$. 注意 $R/(0)\cong R$, 即得 2).

3) 设 P 为 R 的一个包含 N 的素理想，于是 R/P 为整环. 根据本章 §1 定理 2, $R'/\sigma(P) \cong R/P$, $R'/\sigma(P)$ 为整环，所以 $\sigma(P)$ 为素理想. 反之，若 $\sigma(P)$ 为素理想，则同样根据本章 §1 定理 2 可知 $\sigma^{-1}(\sigma(P)) = P$ 为素理想. □

由上可知，一个交换幺环的每个极大理想也是素理想. 但是素理想不一定是极大理想. 极大理想是否存在?

定理 9 *设 R 为一个交换幺环，又设 $a \in R$ 是一个非幂零元，则 R 至少有一个素理想而且不含 a 的任何方幂 a^m, $m \geq 0$.*

证明 设 S 为 R 中一切不包含 $\{a^n \mid n \in \mathbf{N}\}$ 的理想集合. 首先，S 非空，因为 $(0) \in S$. S 按集的包含关系为一偏序集. 设 $\{A_\alpha \mid \alpha \in I\}$ 为 S 的任一个链 (I 为指标集). 令 $A = \bigcup_{\alpha \in I} A_\alpha$. 首先 A 是一个理想. 因为对于任意 $b, c \in A$, 存在 $A_\beta, A_\gamma, \beta, \gamma \in I$ 使得 $b \in A_\beta, c \in A_\gamma$. 因为 $\{A_\alpha \mid \alpha \in I\}$ 是一个链，A_β, A_γ 有包含关系，不妨设 $A_\beta \subset A_\gamma$. 于是 $b - c \in A_\gamma, b - c \in A$, 而且对任意 $x \in R$ 有 $x \cdot b \in A_\beta, x \cdot b \in A$, 所以 A 为一理想. 其次证明 A 不含 $\{a^n \mid n \in \mathbf{N}\}$. 假若 A 包含 a 的某个方幂 $a^m, m \geq 0$, 则 a^m 将含于某个 A_α 中，$\alpha \in I$, 矛盾. 所以 $A \in S$. 于是 S 满足佐恩引理的条件. 根据佐恩引理，S 有一个极大元，设为 P. 求证 P 为素理想. 假若 P 非素理想，则存在元素 $b, c \in R$ 使得 $bc \in P$ 但 $b \notin P, c \notin P$. 令 $H = Rb + P, N = Rc + P$. H, N 为 R 的理想而且 $P \subset H, b \notin H$, 因而 $P \neq H$. 由于 P 为 S 的极大元，因而 $H \notin S$, H 与 $\{a^n \mid n \in \mathbf{N}\}$ 有交，即某个方幂 $a^r \in H$. 同理有某个方幂 $a^s \in N$. 于是 $a^{r+s} \in H \cdot N$. 但是 $H \cdot N = (Rb + P)(Rc + P) = Rbc + RbP + RcP + P^2 \subset P$, 因而 $H \cdot N$ 与 $\{a^m \mid m \in \mathbf{N}\}$ 又无交，矛盾. 所以 P 是一个素理想而且与 $\{a^m \mid m \in \mathbf{N}\}$ 无交. □

推论 1 *一个交换幺环至少有一个极大理想.*

证明 在定理 9 中取 $a = 1$, 求证 P 为极大理想. 设 H 为 R 的一个理想使得 $H \supset P$ 但 $H \neq P$. 由于 P 为 S 的一个极大元，因而 $H \notin S$, H 与 $\{1\}$ 有交，即 $1 \in H$, 于是 $H = R$. 所以 P 为极大. □

推论 2 *设 R 为一个交换幺环，则 R 的全部素理想的交，记作 $r(R)$, 恰好由 R 的全部幂零元组成.*

证明 设 a 为 R 的任一个幂零元，于是 $a^m = 0$ 对某个 $m > 0$. 对 R 的每个素理想 P, 首先有 $a^m = 0 \in P$. 设 r 是最小正整数使得 $a^r \in P$. 若 $r > 1$, 则从 $a^r = a \cdot a^{r-1} \in P$ 得 $a \in P$ 或 $a^{r-1} \in P$, 总之与 r 的取法矛盾. 所以 $r = 1$ 即 $a \in P$. 因此 R 的每个幂零元属于 $r(R)$. 反之，设 a 为 R 的任一个非幂零元，根据定理 9, 存在 R 的一个素理想 P 使得 $a \notin P$, 因而 $a \notin r(R)$. 这就证明了，$r(R)$ 恰好由 R 的全部幂零元组成. □

在推论 2 中定义的理想 $r(R)$ 叫做环 R 的 **诣零根**.

由推论 2 告诉我们这样一个事实：一个交换环 R 的幂零元素全体构成 R 的一个理想. 就是说，若 a,b 为 R 的幂零元，则 $a-b, cb$ $(c\in R)$ 都是幂零元. 不过，这个事实可以给一个直接的证明，不必从推论 2 导出.

例 整数环 $\mathbf{Z}$ 的诣零根是 (0). 任给一个大于 1 的整数 n, $n=p_1^{e_1}\cdots p_r^{e_r}$ 为它的分解式，$e_i\geq 1$. 考察商环 $\mathbf{Z}_n=\mathbf{Z}/(n)$ 的诣零根. 由定理 8,3) 可知 $\mathbf{Z}_n$ 的素理想都是 $\mathbf{Z}$ 中包含 (n) 的素理想在自然同态 $\mathbf{Z}\to\mathbf{Z}_n$ 下的同态象. 不难证明，$\mathbf{Z}$ 中包含 (n) 的素理想为 $(p_1),\cdots,(p_r)$. 因此 $\mathbf{Z}_n$ 的素理想就是 $(p_1)/(n),\cdots,(p_r)/(n)$. 它们的交 $r(\mathbf{Z}_n)=(p_1)/(n)\cap\cdots\cap(p_r)/(n)=(p_1)/(n)\cdots(p_r)/(n)=(p_1\cdots p_r)/(n)$. 这个事实也可以给予一个直接的证明.

§5 商域和分式环

从整数作出有理数的方法可以推广到整环上去. 从一个整环 R 出发可以作出一个商域，即作出一个既包含 R 又是最小的域.

定义 4 设 R 为一整环. 一个域 F 叫做整环 R 的 **商域**, 如果 R 和 F 满足

1) R 是 F 的一个子环;

2) F 的每个元素 a 可以表成 R 的两个元素的商 $a=\dfrac{b}{c}, c\neq 0$.

从定义看出，环 R 交换而且无零因子的条件是必要的. 一个有零因子的交换环不可能作为一个域的子环. 下面按照作有理数的方法从一个整环 R 作出 R 的商域.

设 R 是一个整环， $R^*=R-\{0\}$, R^* 为一个乘法幺半群. 作笛卡尔积 $T=R\times R^*=\{(a,b), a\in R, b\in R^*\}$. 在 T 上定义一个关系 $\sim$:

$$(a,b)\sim(c,d) \text{ 当且仅当 } ad=bc.$$

$\sim$ 显然是反身的和对称的，而且也是传递的. 设

$$(a,b)\sim(c,d),\quad (c,d)\sim(e,f),$$

于是 $ad=bc, cf=de$ 且有 $adf=bcf=bde$, 因为 $d\neq 0$ 且 R 为整环，消去 d 得 $af=be$. 所以 $(a,b)\sim(e,f)$. 作商集 $F=T/\sim$, 含 (a,b) 的类记作 $\dfrac{a}{b}$. 于是 $\dfrac{a}{b}=\dfrac{c}{d}\iff ad=bc$. 在 F 中定义运算

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},$$

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}.$$

定义与类的代表取法无关. 因为, 设 $\frac{a'}{b'}=\frac{a}{b},\frac{c'}{d'}=\frac{c}{d}$, 则有

$$\frac{a'}{b'}+\frac{c'}{d'}=\frac{a'd'+b'c'}{b'd'}=\frac{ad'+bc'}{bd'}=\frac{ad+bc}{bd}=\frac{a}{b}+\frac{c}{d}.$$

仿上可知 $\frac{a'}{b'}\cdot\frac{c'}{d'}=\frac{a}{b}\cdot\frac{c}{d}$. F 对加法和乘法成一个域. 加法和乘法的结合律、交换律和分配律由读者自己去验证. 我们指出 $\frac{0}{b}$ 是 F 的零元素, 简记作 0. $-\frac{a}{b}=\frac{-a}{b}$ 为 $\frac{a}{b}$ 的负元素. $\frac{b}{b}$ 是 F 的单位元素, 简记作 1. 若 $\frac{a}{b}\neq 0$, 则 $\left(\frac{a}{b}\right)^{-1}=\frac{b}{a}$. 其次, F 包含一个子环 $R'=\left\{\frac{a}{1}\middle| a\in R\right\}$. F 中元素 $\frac{a}{b}$ 可写成 R' 中元素的商 $\frac{a}{b}=\frac{a}{1}\Big/\frac{b}{1}$. 映射 $a\mapsto\frac{a}{1}$ 是 R 到 F 的一个嵌入, 将 $\frac{a}{1}$ 与 a 等同, R 与 F 的子环等同. 则 F 的元素可写成 R 中元素的商. 所以 F 是 R 的一个商环, 即得

定理 10 每个整环有一个商域. □

其次证明商域的唯一性.

定理 11 设 R 为一整环, F 为它的一个商域. 则 R 到一个域 F' 的任一个单一同态 η 恒可以唯一地扩充成 F 到 F' 的一个单一同态.

证明 首先证明存在性. 设 $T=\{(a,b)\,|\,a,b\in R,b\neq 0\}$. 定义映射 $\xi:T\to F'$ 如下

$$\xi(a,b)=\eta(a)\cdot\eta(b)^{-1}.$$

若 $(a,b)\sim(c,d)$, 则 $ad=bc$, $\eta(a)\eta(d)=\eta(b)\eta(c)$. 从而 $\xi(a,b)=\xi(c,d)$. 反之, 从 $\xi(a,b)=\xi(c,d)$ 可知 $(a,b)\sim(c,d)$. 因此, ξ 确定了商集 $F=T/\sim$ 到 F' 的一个单一映射 η':

$$\eta'\left(\frac{a}{b}\right)=\xi(a,b)=\eta(a)/\eta(b).$$

η' 显然保持运算. 因而 η' 是 F 到 F' 的一个单一同态而且是 η 的一个扩充.

其次证明 η' 的唯一性. 设 η'' 是一个 η 在 F 上的任一个扩充. 求证 $\eta''=\eta'$. 对于任一元素 $x\in F$, x 可以表成 $x=a\cdot b^{-1},a,b\in R$. 于是 $xb=a$, 将 η' 和 η'' 分别作用于等式, 一方面从 $\eta'(xb)=\eta'(a)$ 得 $\eta'(x)\eta(b)=\eta(a)$. 另一方面从 $\eta''(xb)=\eta''(a)$ 得 $\eta''(x)\eta(b)=\eta(a)$, 从而 $\eta''(x)=\eta'(x)$(注意 $\eta(b)\neq 0$). 从而 $\eta''=\eta'$. □

推论 一个整环 R 的商域在同构意义下是唯一的.

证明 设 F 和 F' 为 R 的两个商域, 根据定理 11, 存在一个单一同态 η': $F\to F'$ 而且保持 R 的元素映到自己. 又因 F' 是 R 的商域, F' 的每个元素 $x'=ab^{-1},a,b\in R$, 是 F 中元素 $x=ab^{-1}$ 在 η' 下的象. 因而 η' 是满射. 所以 η' 是 F 到 F' 的一个同构而且保持 R 的元素不动. □

从整环作出它的商域这种思想可以从几个方面加以推广. 一是放弃无零因子的条件, 一是放弃交换条件或者甚至两者都放弃. 我们在这里扼要地介绍前一种推广, 即局部化方法. 它是研究环的一个侧面的方法, 有如研究一条曲线在一点的局部行为.

设 R 为一个有单位元素的交换环. R 的一个非空子集 S 叫做 **乘性子集**, 如果 S 对乘法封闭, 即若 $s_1, s_2 \in S$, 则 $s_1 \cdot s_2 \in S$. R 的一个乘性子集 S 确定 R 的一个理想 $N = \{a \in R \mid \text{存在 } s \in S \text{ 使得 } as = 0\}$. 首先, N 是一个加法子群. 因为对于 $a_1, a_2 \in N$, 存在 $s_1, s_2 \in S$ 使得 $a_1 s_1 = a_2 s_2 = 0$. 于是 $(a_1 - a_2)s_1 s_2 = 0$ 而且 $s_1 s_2 \in S$, 因而 $a_1 - a_2 \in N$. 显然对任意 $x \in R, a \in N$ 恒有 $xa \in N$. 所以 N 是 R 的一个理想.

若 S 含零元素 0, 则 $N = R$. 若 S 不含 0, 则 $N \cap S = \emptyset$. 因为假若 $N \cap S$ 非空, 取一个 $a \in N \cap S$, 于是存在一个 $s \in S$ 使 $as = 0$. 但是 S 乘法封闭, 从 $a, s \in S$ 有 $as = 0 \in S$, 矛盾. 若 S 不含 R 的零因子, 则 $N = \{0\}$.

定义 5 设 R 为一个交换幺环, S 为 R 的一个乘性子集, N 为由 S 如上定义的 R 的理想. 如果一个有单位元素 $1'$ 的交换环 R' 满足下列条件:

1) 存在一个环同态 $\sigma: R \to R'$ 使得 $\sigma(1) = 1'$, 而且对任一 $s \in S, \sigma(s)$ 在 R' 内有逆;

2) $\ker(\sigma) = N$;

3) R' 的每个元素 x 可表成 $x = \sigma(a)/\sigma(s)$, 其中 $a \in R, s \in S$:

则 R' 叫做 R 关于乘性子集 S 的 **分式环**. 以后 R' 记作 $S^{-1}R$.

若 S 含零元素, 则 $N = R, S^{-1}R = \{0\}$. 以下假定 S 不含零元素.

定理 12 *设 R 为一个交换幺环, S 为 R 的任一乘性子集, 而且 $0 \notin S$. 于是 R 关于 S 的分式环存在.*

证明 设 N 为由 S 确定的 R 的理想. 作 R 与 S 的笛卡尔积 $T = \{(a,s) \mid a \in R, s \in S\}$. 在 T 上定义关系 "$\sim$" 如下

$$(a,s) \sim (a',s') \iff as' - a's \in N.$$

"$\sim$" 显然是反身的、对称的. 证明它也是传递的. 设 $(a_1,s_1) \sim (a_2,s_2), (a_2,s_2) \sim (a_3,s_3)$. 于是

$$a_1 s_2 - a_2 s_1 \in N, \quad a_2 s_3 - a_3 s_2 \in N.$$

于是 $s_3(a_1 s_2 - a_2 s_1) + s_1(a_2 s_3 - a_3 s_2) = s_2(a_1 s_3 - a_3 s_1) \in N$. 根据 N 的定义, 存在一个 $s \in S$ 使 $ss_2(a_1 s_3 - a_3 s_1) = 0$. 由于 S 对乘法封闭, $ss_2 \in S$, 从而 $a_1 s_3 - a_3 s_1 \in N$, 所以 $(a_1,s_1) \sim (a_3,s_3)$. 商集 $T/\sim$ 记作 $S^{-1}R$, 包含 (a,s) 的等价类记作 $\overline{(a,s)} = \frac{a}{s}$. 于是 $\frac{a_1}{s_1} = \frac{a_2}{s_2} \iff a_1 s_2 - a_2 s_1 \in N$. 在 $S^{-1}R$ 内定义加

法和乘法:

$$\frac{a_1}{s_1}+\frac{a_2}{s_2}=\frac{a_1s_2+a_2s_1}{s_1s_2},$$

$$\frac{a_1}{s_1}\cdot\frac{a_2}{s_2}=\frac{a_1a_2}{s_1s_2}.$$

不难验证定义和类的代表的取法无关，而加法和乘法满足环的条件，因而 $S^{-1}R$ 成一环. $\frac{0}{s}=\frac{0}{s'}$ 为零元素，简记作 0. $\frac{s}{s}=\frac{s'}{s'}$ 为单位元素，简记作 $1'$. 映射 $\sigma: R\to S^{-1}R$ 规定为 $\sigma(a)=\frac{as}{s}$. 显然 $\sigma(1)=1'$ 而且 σ 是一个环同态. 决定 $\ker(\sigma)$, $\frac{as}{s}=0 \iff \frac{as}{s}=\frac{0}{s'} \iff ass'\in N$. 而 $ass'\in N \iff a\in N$. 所以 $\ker(\sigma)=N$. 对于 S 的元素 s. $\sigma(s)=\frac{ss'}{s'}$ 在 $S^{-1}R$ 内有逆元 $\frac{s'}{ss'}$. 最后 $S^{-1}R$ 的元素 $\frac{a}{s}$ 可以表成

$$\frac{a}{s}=\frac{as'}{ss'}=\frac{as'}{s'}\cdot\frac{s'}{ss'}=\sigma(a)\cdot\sigma(s)^{-1}.$$

这就完全证明了 R 关于乘性子集 S 的分式环的存在性. □

当 R 为整环时，若取 $S=R^*=R-\{0\}$, 则 $S^{-1}R$ 就是 R 的商域，因为此时 $N=(0)$.

说明 σ 是单一同态的充要条件是 $N=(0)$. 而 $N=(0)$ 的充要条件是 S 不含 R 的零因子. 稍弱一点， σ 限制在 S 上为单射的充要条件是在 S 内乘法消去律成立，即从 $s(s_1-s_2)=0(s,s_1,s_2\in S)$, 恒有 $s_1=s_2$.

分式环和商域一样有它的通用性而且在同构意义下是唯一的. 我们在下面给出它而不加证明.

定理 13 *设 R 为一个交换幺环， S 为它的一个乘性子集. 设 η 是 R 到交换幺环 R' 的一个同态使得 $\eta(1)=1'$, 而且对任一 $s\in S$, $\eta(s)$ 在 R' 内有逆元，则 η 可以唯一地开拓成环同态 $\xi: S^{-1}R\to R'$ 使得 η 分解成 $\eta=\xi\sigma$, 其中 σ 为定理 12 的证明所给的标准同态 $R\to S^{-1}R$.*

推论 *交换幺环 R 关于乘性子集 S 的分式环在同构意义下是唯一的.* □

例 设 p 为整数环 $\mathbf{Z}$ 的一个素数. (p) 为 $\mathbf{Z}$ 的一个素理想，令 $S=\mathbf{Z}-(p)$. 则 S 由所有与 p 互素的整数组成，因而 S 是一个乘性子集. 此时 $N=(0)$, 标准同态 $\sigma:\mathbf{Z}\to S^{-1}\mathbf{Z}$ 是单一的. 因此，可以将整数 a 与 $\sigma(a)$ 等同. 于是 $\mathbf{Z}\subset S^{-1}\mathbf{Z}$, 整数 a 在 $S^{-1}\mathbf{Z}$ 中有逆的充要条件是 a 与 p 互素. $S^{-1}\mathbf{Z}$ 的元素可写成

$$x=\frac{r}{s}\cdot p^t,$$

其中 $r,s\in\mathbf{Z},(r\cdot s,p)=1,t$ 为非负整数. x 为 $S^{-1}\mathbf{Z}$ 的单位当且仅当 $t=0$.

$S^{-1}\mathbf{Z}$ 有唯一的一个非零素理想 P 即

$$P=\{xp\,|\,x\in S^{-1}\mathbf{Z}\}.$$

$S^{-1}\mathbf{Z}$ 的非零非单位理想都是 P 的某个正整数幂 P^m、$m\geq 1$. 研究这种分式环就等于研究整数环的一个局部情况.

§6 交换环上的多项式环

这一节和前两节一样, 讨论的环只限于交换幺环. 若环 R 是环 R' 的子环, 则 R' 称为 R 的扩环. 谈到环 R 的扩环 R' 时总假定 R 和 R' 有相同的单位元素. 本节的目的是利用多项式环来研究有限生成环的结构. 有限生成是构造环的一种较普遍的方法.

设 R 为一个交换幺环, R' 为 R 的一个扩环, 交换而且与 R 有相同的单位元素. 在 R' 内任取一个元素 u, 考虑所有形如下列元素

$$a_0+a_1u+a_2u^2+\cdots+a_nu^n,\ a_i\in R, n\geq 0.$$

的集合, 记作 $R[u]$. 首先 $R[u]$ 是 R' 的加法子群. 运用乘法交换律和分配律, $R[u]$ 的元素相乘可如下进行

$$\left(\sum_{i=0}^{n}a_iu^i\right)\left(\sum_{j=0}^{m}b_ju^j\right)=\sum_{i=0}^{n}\sum_{j=0}^{m}a_ib_ju^{i+j}=\sum_{k=0}^{m+n}c_ku^k,$$

其中 $c_k=\sum\limits_{i+j=k}a_ib_j$, $k=0,1,\cdots,m+n$. 因而 $R[u]$ 对乘法是封闭的. 所以 $R[u]$ 是 R' 的一个子环. 显然 $R\subset R[u]$ 而且 $u\in R[u]$(因为 R' 与 R 有相同的单位元素).$R[u]$ 叫做元素 u 在 R 上 **生成** 的子环. $R[u]$ 的元素叫做 u 在 R 上的多项式. 确定 $R[u]$ 的结构, 首先要确定 u 的两个多项式相等的条件, 或者说确定 u 的一个多项式等于零的条件. 若 u 的一个多项式 $a_0+a_1u+\cdots+a_nu^n=0$, 则它叫做 u 在 R 上的一个 **代数关系**. $R[u]$ 的结构由 u 在 R 上的代数关系总和来决定. 为了确定 $R[u]$ 的结构, 首先作一个 R 的扩环使得它包含一个元素 x, 它在 R 上只有平凡的代数关系.

定义 6 设 R 为一个交换幺环. 用 $R[[x]]$ 表示一切无限序列

$$(a_n)=(a_0,a_1,a_2,\cdots),\ a_i\in R,\ i=0,1,2,\cdots$$

组成的集合. 在 $R[[x]]$ 内定义 + 和 · 如下

$$(a_n)+(b_n)=(a_n+b_n),$$
$$(a_n)\cdot(b_n)=(c_n),$$

其中 $c_n = a_0b_n + a_1b_{n-1} + \cdots + a_nb_0 = \sum\limits_{i+j=n} a_ib_j$. 于是 $R[[x]]$ 成一环, 叫做 R 上的 **一元形式幂级数环**. 验证 $R[[x]]$ 是一个环, 作为练习留给读者.

$R[[x]]$ 是一个有单位元素 $1 = (1, 0, \cdots,)$ 的交换环. 它包含 $R_0 = \{(a_0, 0, \cdots) \mid a_0 \in R\}$ 作为子环. R 与 R_0 同构, 此同构由 $a_0 \mapsto (a_0, 0, 0, \cdots)$ 给出. 将 a_0 与 $(a_0, 0, 0, \cdots)$ 等同, 于是 R 为 $R[[x]]$ 的子环, 而且 $a \cdot (a_n) = (aa_0, aa_1, \cdots), a \in R$.

定义 7 在 $R[[x]]$ 中取 $x = (0, 1, 0, 0, \cdots)$. 于是 x 在 R 上生成的子环 $R[x]$ 叫做 R 上的 **一元多项式环**.

对于 $i = 0, 1, 2, \cdots$, 由计算可知 $x^i = (0, \cdots, 0, 1, 0, \cdots)$, 其中的 1 位于第 $i+1$ 分量处, 因而 $R[x]$ 中每个元素可表成

$$a_0 + a_1x + \cdots + a_nx^n = (a_0, a_1, \cdots, a_n, 0, 0, \cdots).$$

由此可知, $a_0 + a_1x + \cdots + a_nx^n = 0$ 的充要条件是所有系数 $a_0, a_1, \cdots, a_n$ 全为 0. 从而可知 x 的两个多项式 $a_0 + a_1x + \cdots$ 和 $b_0 + b_1x + \cdots$ 相等的充要条件是对应系数一一相等 $a_i = b_i, i = 0, 1, \cdots$. 因此 x 叫做 R 上的一个 **未定元**. 以后 x 在 R 上的多项式用 $f(x), g(x), h(x)$ 等表示.

下面的定理说明环上由一个元素生成的环总是多项式环的同态象.

定理 14 设 σ 为环 R 到环 S 的一个同态而且 $\sigma(1) = 1'$, 这里 $1'$ 是 S 的单位元素, 则对任一元素 $u \in S$, σ 恒可唯一地扩充成 R 上未定元 x 的多项式环 $R[x]$ 到 S 的同态 σ_u, 使得 $\sigma_u(x) = u$.

证明 对 $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$, 作 $R[x]$ 到 S 的映射 σ_u

$$\sigma_u(f(x)) = \sigma(a_0) + \sigma(a_1)u + \cdots + \sigma(a_n)u^n,$$

首先, 这个定义是合理的, 就是说, 从 $f(x) = g(x)$ 不难推出 $\sigma_u(f(x)) = \sigma_u(g(x))$. 设 $g(x) = b_0 + b_1x + \cdots + b_mx^m$. 容易验证 $\sigma_u(f(x) + g(x)) = \sigma_u(f(x)) + \sigma_u(g(x))$. 其次验证 σ_u 也保持乘法. 设 $f(x)g(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}$. 其中 $c_i = \sum\limits_{\nu+\mu=i} a_\nu b_\mu$. 于是

$$\begin{aligned}\sigma_u(f(x) \cdot g(x)) &= \sigma_u(c_0 + c_1x + \cdots + c_{n+m}x^{n+m}) \\ &= \sigma(c_0) + \sigma(c_1)u + \cdots + \sigma(c_{n+m})u^{n+m},\end{aligned}$$

其中 $\sigma(c_i) = \sigma\left(\sum\limits_{\nu+\mu=i} a_\nu b_\mu\right) = \sum\limits_{\nu+\mu=i} \sigma(a_\nu)\sigma(b_\mu)$, 所以

$$\sigma_u(f(x) \cdot g(x)) = \sigma_u(f(x)) \cdot \sigma_u(g(x)).$$

而且

$$\sigma_u(x) = \sigma(1)u = 1' \cdot u = u,$$
$$\sigma_u(a) = \sigma(a), \quad a \in R.$$

所以 σ_u 是 σ 在 $R[x]$ 上的一个扩充，而且 $\sigma_u(x) = u$. σ_u 显然由 σ 和 x 的象唯一决定，$R[x]$ 在 σ_u 下的象为 $\sigma(R)[u]$. □

推论 设 S 为 R 的一个扩环且与 R 有相同的单位元素，对任一 $u \in S$，存在 $R[x]$ 的一个理想 I 使得

$$R[u] \cong R[x]/I, \quad \text{且 } I \cap R = \{0\}.$$

证明 在定理 14 中取 σ 为 R 到 S 的包含映射 $\sigma(a) = a$, $a \in R$. 于是存在 $R[x]$ 到 S 的同态 σ_u，使得 $\sigma_u(x) = u$ 而且 σ_u 限制在 R 上为恒等映射. 设 $\ker(\sigma_u) = I$，于是

$$R[u] \cong R[x]/I.$$

由于 σ_u 在 R 上为恒等映射，$I \cap R = \{0\}$. □

说明 在推论中 $f(x) \in I$ 的充要条件是 $f(u) = 0$，因此，I 是元素 u 在 R 上的代数关系的总和，若 $I = (0)$，则 u 在 R 上只有一个平凡代数关系 $0 + 0 \cdot u + \cdots = 0$，则称 u 在 R 上是 **超越的**，此时也称 u 是 R 上的 **超越元**. 若 $I \neq (0)$，则 I 包含一个非零多项式 $f(x)$ 使得 $f(u) = 0$，则称 u 在 R 上是 **代数的**. 此时也称 u 是 R 上的 **代数元**，同时称 u 是多项式 $f(x)$ 的 **根**.

其次，考虑推论的逆. 设 I 为 $R[x]$ 的一个理想使得 $I \cap R = \{0\}$，则自然同态 $R[x] \to R[x]/I$ 限制在 R 上为一个单一同态. 因此，R 可以嵌入 $S = R[x]/I$ 内，R 作为 S 的子环且有相同的单位元素. 将 $x + I$ 记成 u. 则 S 是在 R 上添加 u 所生成的环，因此研究环 $R[u]$ 的构造问题就归结为研究 $R[x]$ 的满足 $I \cap R = \{0\}$ 的理想 I 的问题.

下面将环上一元多项式环推广到环上多元多项式环. 设 R 为一个有单位元素的交换环，n 为任一个正整数. 我们归纳地定义 R 上 n **个未定元** $x_1, \cdots, x_n$ **的多项式环**(记作 $R[x_1, \cdots, x_n]$) 如下：当 $n = 1$ 时 $R[x_1]$ 已在上面定义 (定义 7). 当 $n > 1$ 时，定义 $R[x_1, \cdots, x_n]$ 为

$$R[x_1, \cdots, x_n] = R[x_1, \cdots, x_{n-1}][x_n].$$

它是一个有单位元素的交换环，包含 R 作为子环. $R[x_1, \cdots, x_n]$ 的元素可写成

$$f(x_1, \cdots, x_n) = \sum_{i=0}^{r} f_i(x_1, \cdots, x_{n-1}) x_n^i.$$

其中 $f_i(x_1,\cdots,x_{n-1})\in R[x_1,\cdots,x_{n-1}]$. 每个 $f_i(x_1,\cdots,x_{n-1})$ 又可写成 x_{n-1} 的多项式, 系数属于 $R[x_1,\cdots,x_{n-2}]$. 如此继续下去, $f(x_1,\cdots,x_n)$ 最后可写成有限和形式

$$f(x_1,\cdots,x_n)=\sum_{i_1,\cdots,i_n>0}a_{i_1\cdots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n},$$

因此每个 $f(x_1,\cdots,x_n)$ 是一些单项式 $a_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}$ 的有限和. $f(x_1,\cdots,x_n)=0$ 的充要条件是所有 $f_i(x_1,\cdots,x_{n-1})$ 都等于零. 应用归纳法 (对 n 作归纳) 可知 $f(x_1,\cdots,x_n)=0$ 的充要条件是所有系数 $a_{i_1\cdots i_n}=0$. 这是刻画 $x_1,\cdots,x_n$ 为 R 上独立未定元的唯一条件.

设 R' 为 R 的一个扩环, R' 交换而且和 R 有相同的单位元素, $u_1,\cdots,u_n$ 为 R' 中任意 n 个元素. 对于每个 $f(x_1,\cdots,x_n)\in R[x_1,\cdots,x_n]$, 用 u_i 代入 x_i 就得到 R' 的一个元素 $f(u_1,\cdots,u_n)$, 叫做 $u_1,\cdots,u_n$ 的一个多项式. 不难看出这种代入是合理的, 就是说, 从 $f(x_1,\cdots,x_n)=g(x_1,\cdots,x_n)$ 推出 $f(u_1,\cdots,u_n)=g(u_1,\cdots,u_n)$. 其次对于任意两个 $f(x_1,\cdots,x_n),g(x_1,\cdots,x_n)\in R[x_1,\cdots,x_n]$ 恒有

$$(f+g)(u_1,\cdots,u_n)=f(u_1,\cdots,u_n)+g(u_1,\cdots,u_n),$$
$$(f\cdot g)(u_1,\cdots,u_n)=f(u_1,\cdots,u_n)\cdot g(u_1,\cdots,u_n).$$

由此可知集合 $R[u_1,\cdots,u_n]=\{f(u_1,\cdots,u_n)\,|\,f(x_1,\cdots,x_n)\in R[x_1,\cdots,x_n]\}$ 是 R' 的一个子环, 而且包含 R. $R[u_1,\cdots,u_n]$ 叫做**元素 $u_1,\cdots,u_n$ 在 R 上生成的子环**, 一般叫做 **R上的有限生成环**. 而且同时也证明了映射 $f(x_1,\cdots,x_n)\mapsto f(u_1,\cdots,u_n)$ 是 $R[x_1,\cdots,x_n]$ 到 $R[u_1,\cdots,u_n]$ 的环同态. 但是我们有更一般的结果

定理 15 设 R 为一个交换幺环, $R[x_1,\cdots,x_n]$ 为 R 上 n 个未定元 $x_1,\cdots,x_n$ 的多项式环. 又设 S 为一个交换幺环, $u_1,\cdots,u_n$ 为 S 中任意给定的 n 个元素, σ 为 R 到 S 的一个环同态而且 $\sigma(1)=1'$. 则 σ 可以唯一地扩充成 $R[x_1,\cdots,x_n]$ 到 S 的同态 σ_n 使得 $\sigma_n(x_i)=u_i$, $i=1,\cdots,n$.

证明 应用定理 14, 对 n 作归纳法即得本定理. □

推论 1 设 S 为 R 的扩环, 交换而且与 R 有相同的单位元素. 对于 S 的任意 n 个元素 $u_1,\cdots,u_n$ 存在一个唯一的同态 $\sigma:R[x_1,\cdots,x_n]\to S$ 使得 σ 限制在 R 上为恒等映射, 而且 $\sigma(x_i)=u_i$, $i=1,\cdots,n$. 令 $I=\ker(\sigma)$, 则

$$R[x_1,\cdots,x_n]/I\cong R[u_1,\cdots,u_n],$$

而且 $I\cap R=(0)$.

证明 首先 σ 是 R 的恒等映射在 $R[x_1,\cdots,x_n]$ 上的扩充. 这里只需要证明 $I\cap R=(0)$. 设 $a\in I\cap R$. 一方面由于 $a\in I,\sigma(a)=0$; 另一方面, 由于

$a \in R, \sigma(a) = a$, 所以 $a = 0$, 即 $I \cap R = (0)$. □

说明 在推论 1 中 R 上有限生成子环 $R[u_1, \cdots, u_n]$ 的结构决定于理想 I. 对任一 $f(x_1, \cdots, x_n) \in I$, 有 $f(u_1, \cdots, u_n) = 0$. $f(x_1, \cdots, x_n)$ 叫做元素 $u_1, \cdots, u_n$ 在 R 上的一个 **代数关系**. I 就是 $u_1, \cdots, u_n$ 在 R 上的代数关系的总和. 当 $I = (0)$ 时, 对任一 $f(x_1, \cdots, x_n) \in R[x_1, \cdots, x_n]$, $f(u_1, \cdots, u_n) = 0$ 的充要条件是 $f(x_1, \cdots, x_n) = 0$. 在这种情况, $u_1, \cdots, u_n$ 叫做 R 上的 **代数无关元**, 也叫做在 R 上是 **代数无关的**. 否则 $u_1, \cdots, u_n$ 叫做在 R 上是 **代数相关的**.

推论 2 设 N 为 R 的一个理想, 令 $\overline{R} = R/N$. 设 $\overline{R}[y_1, \cdots, y_n]$ 为 $\overline{R}$ 上的 n 个未定元 $y_1, \cdots, y_n$ 的多项式环. 于是 $R[x_1, \cdots, x_n]/N[x_1, \cdots, x_n] \cong \overline{R}[y_1, \cdots, y_n]$. 特别, 若 N 为 R 的素理想, 则 $N[x_1, \cdots, x_n]$ 是 $R[x_1, \cdots, x_n]$ 的素理想. 这里, $N[x_1, \cdots, x_n]$ 表示 $R[x_1, \cdots, x_n]$ 中系数属于 N 的多项式全体.

证明 根据定理 15, 自然同态 $\sigma : R \to \overline{R}$ 可以唯一地扩充成 $\sigma_n : R[x_1, \cdots, x_n] \to \overline{R}[y_1, \cdots, y_n]$ 使得 $\sigma_n(x_i) = y_i$, $i = 1, \cdots, n$. $R[x_1, \cdots, x_n]$ 的元素 $f(x_1, \cdots, x_n)$ 属于 $\ker(\sigma_n)$ 的充要条件是 $f(x_1, \cdots, x_n)$ 的每个单项式的系数都属于 N, 即 $f(x_1, \cdots, x_n) \in N[x_1, \cdots, x_n]$. 所以 $\ker(\sigma_n) = N[x_1, \cdots, x_n]$. 其次, 若 N 为 R 的素理想, 则 $\overline{R}$ 为整环. 读者对 n 作归纳法不难证明 $\overline{R}[y_1, \cdots, y_n]$ 也是一个整环 (这一点在下一节还要谈到), 因而根据定理 8, 可知 $N[x_1, \cdots, x_n]$ 是 $R[x_1, \cdots, x_n]$ 的素理想. □

说明 对定理 15, 推论 1 后面的说明再补充一点. 环 R 上的有限生成环 $R[u_1, \cdots, u_n]$ 的结构决定于多项式环 $R[x_1, \cdots, x_n]$ 的理想 I. I 是 $u_1, \cdots, u_n$ 在 R 上一切代数关系的总和. 但 I 包含的多项式多至无限. 是否存在有限多个基本的代数关系使得其它的代数关系都是这些基本关系的组合, 系数属于 $R[x_1, \cdots, x_n]$? 如果是这样, 对于 $R[u_1, \cdots, u_n]$ 的研究无疑是一个很大的推进. 这问题牵涉到多项式环 $R[x_1, \cdots, x_n]$ 的理想是否是有限生成的? 当 R 为一域或整数环时, 答案是肯定的. 这将在下章讨论.

§7 整环上的一元多项式环

这一节讨论整环上的一元多项式的根的一些性质, 也就是讨论整环上的代数元的某些性质, 特别是域上代数元的性质.

设 R 为一个交换幺环, $R[x]$ 为 R 上的一元多项式环. 设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$. 如高等代数中一样, 若 $a_n \neq 0$, 则 n 叫做 $f(x)$ 的 **次数**, 记作 $n = \deg f(x)$. 0 的次数规定为 $-\infty$. 由定义, 非零常数 $a = ax^0$ 的次数

为 0. 不难验证次数有如下性质:

$$\deg(f(x)+g(x)) \le \max(\deg f(x), \deg g(x)),$$
$$\deg(f(x)g(x)) \le \deg f(x) + \deg g(x).$$

当 $\deg f(x) \neq \deg g(x)$ 时, 第一式的等号成立; 当 $f(x)$ 或 $g(x)$ 的首项系数不是零因子时, 第二式的等号成立.

设 R 为整环, 则有

$$\deg(f(x)\cdot g(x)) = \deg f(x) + \deg g(x).$$

若 $f(x)\cdot g(x)=1$, 则 $\deg f(x)+\deg g(x)=0$. 从而 $\deg f(x)=\deg g(x)=0$. $f(x)$ 和 $g(x)$ 只能是非零常数. 因而它们都是 R 中单位. 因此得

定理 16 若 R 为一整环, 则 $R[x]$ 也是整环而且 $R[x]$ 的单位群与 R 的单位群相等.

推论 若 R 为整环, 则多元多项式环 $R[x_1,\cdots,x_n]$ 也是整环, 而且它的单位群与 R 的相同.

数域上一元多项式的除法算式可推广成:

定理 17 (除法算式) 设 R 为一个交换环, $f(x), g(x) \in R[x]$, $g(x) \neq 0$, 而且 $g(x)$ 的首项系数为单位, 于是存在唯一的一对多项式 $q(x), r(x) \in R[x]$ 使得

$$f(x) = q(x)\cdot g(x) + r(x),$$
$$\deg r(x) < \deg g(x).$$

推论 1 (余数定理) 设 $f(x) \in R[x], c \in R$, 则 $f(x)$ 可表成

$$f(x) = q(x)\cdot(x-c) + f(c).$$

在定理 17 中若 $r(x)=0$, 则称 $g(x)$**整除**$f(x)$, 记成 $g(x)|f(x)$, 此时 $g(x)$ 叫做 $f(x)$ 的**因式**, $f(x)$ 叫做 $g(x)$ 的**倍式**.

推论 2 (因式定理) 设 $c \in R, f(x) \in R[x]$, 则 $(x-c)|f(x)$ 的充要条件是 c 为 $f(x)$ 的一根.

定理 17 及其推论的证明和 R 为数域的情况完全一样.

定理 18 设 R 为一整环, $f(x) \in R[x], \deg f(x) = n \ge 0$, 则 $f(x)$ 在 R 内最多有 n 个不同的根.

证明 设 F 为 R 的商域, 把 $f(x)$ 看作 $F[x]$ 的多项式, 证明完全与数域的情况类似. □

定理 18 中 R 的交换性和无零因子这两个条件是必要的. 举例如下:

例 1 设 H 为实数域 $\mathbf{R}$ 上四元数体. $f(x)=x^2+1$ 在 H 内至少有 3 根 I,J,K. 实际上, $f(x)$ 在 H 内有无穷多个根. 这种情况的出现是由于 H 的乘法不交换. 对于任一元素 $\alpha\in H, \alpha I\alpha^{-1}$ 都是 $f(x)$ 的根. 而且 $\alpha I\alpha^{-1}=\beta I\beta^{-1}\iff\beta^{-1}\alpha\in\mathbf{R}[I]$.

例 2 在 $\mathbf{Z}/(8)$ 中 x^2-1 有四个根 $\overline{1},\overline{-1},\overline{3},\overline{-3}$. 这种情况的出现是因为 $\mathbf{Z}/(8)$ 中有非零的幂零元. 除 $\overline{\pm 1}$ 外, $\overline{\pm 1}+\overline{4}$ 也是 x^2-1 的根.

例 3 在 $\mathbf{Z}/(15)$ 中 x^2-1 有四个根 $\overline{1},\overline{4},\overline{11},\overline{14}$. 这是因为 $\mathbf{Z}/(15)$ 有零因子. 实际上, $\mathbf{Z}/(15)\cong\mathbf{Z}/(3)\oplus\mathbf{Z}/(5)$. x^2-1 在每个直和项中有两根, 根据孙子定理 x^2-1 有四根.

定理 19 *设 R 为一整环, $R^*=R-\{0\}$ 为一乘法幺半群. 则 R^* 的任一有限子群都是循环的.*

证明 设 G 为 R^* 的一个有限群, 阶 $=n$. G 是一个阿贝尔群, 对 n 的每个因子 d, 根据定理 18,x^d-1 在 R 内最多有 d 个不同的根, 因此 G 中最多有 d 个元素, 其阶整除 d, 根据第二章定理 7,G 是一个循环群. □

注意, 此定理中 "整环" 的条件是必要的.

例 4 在例 1 中, $\{\pm 1,\pm I,\pm J,\pm K\}$ 是一个 8 阶有限群但非循环.

例 5 在例 2 中 $\{\overline{1},\overline{3},\overline{5},\overline{7}\}$ 是 4 阶群但非循环.

在这里应特别提一下有限域, 设 F 为一个有限域, 含 q 个元素, F 的非零元素全体组成一个 $q-1$ 阶乘法群, 记作 F^*, 根据定理 19,F^* 是一个循环群, 于是得

推论 *设 F 为含 q 个元素的有限域, F 中非零元素组成的乘法群 F^* 是一个 $q-1$ 阶循环群. 因此 F 中的元素恰好是方程 $x^q-x=0$ 的全部根.*

设 p 为整数环 $\mathbf{Z}$ 的一个素数, 已知商环 $\mathbf{F}_p=\mathbf{Z}/(p)$ 是一个含 p 个元素的域, 乘法群 $\mathbf{F}_p^*$ 是 $p-1$ 阶循环群. 设 $\overline{a}$ 为 $\mathbf{F}_p^*$ 的一个生成元, a^k 的阶为 $p-1$ 的充要条件是 $(k,p-1)=1$, 因而 $\mathbf{F}_p$ 有 $\varphi(p-1)$ 个生成元, $\varphi(n)$ 为欧拉函数. 在自然同态 $\mathbf{Z}\to\mathbf{F}_p$ 下, 可知 $\overline{a}$ 的任一反象 a 是 $\bmod p$ 的一个 **原根**, 即 $a \bmod p$ 的指数为 $p-1$ 因而整数 $\bmod p$ 有 $\varphi(p-1)$ 个不同的原根.

最后研究域上代数元的性质, 它与域上一元多项式环有密切关系, 数域上的一元多项式环的整除理论对任意域上一元多项式环仍然有效. 因为除法算式 (定理 17) 是它们的共同基础.

定义 8 一个整环 R 叫做 **主理想整环**, 如果 R 的每个理想都是主理想.

例如, 整数环 $\mathbf{Z}$ 是一个主理想整环.

定理 20 *域上的一元多项式环是主理想整环.*

证明 设 $F[x]$ 为域 F 上一元多项式环, N 为任一理想, 零理想显然是主理想, 因而可设 $N\neq(0)$. 于是在 N 的非零元素中取一个次数最低的多项式 $f(x)$.

证明 $N=(f(x))$. 显然 $(f(x))\subset N$, 反之，设 $g(x)\in N$, 作除法算式

$$g(x)=q(x)\cdot f(x)+r(x),$$
$$\deg r(x)<\deg f(x).$$

因 N 为理想，$r(x)=g(x)-q(x)\cdot f(x)\in N$, 根据 $f(x)$ 的选择，$r(x)=0$, 于是 $g(x)\in(f(x)).N\subset(f(x))$, 所以 $N=(f(x))$. □

说明 理想 N 的生成元 $f(x)$ 还可如此取使得 $f(x)$ 的首项系数为 1, 因为如 $f(x)$ 为 N 的一个生成元, 则任一 $cf(x)$ $(c\in F, c\neq 0)$ 也是 N 的生成元. 可适当取 c 使得 $f(x)$ 的首项系数为 1, 这种生成元由 N 唯一决定. 因为 $f(x), g(x)$ 为 N 的任意两个生成元, 首项系数都为 1, 于是 $f(x), g(x)$ 互相整除, 从而 $f(x)=g(x)$.

设 S 为域 F 的一个扩环 (交换) 而且和 F 有相同的单位元素. 设 $u\in S$ 为 F 上的代数元, 根据定理 14 的推论,

$$F[u]\cong F[x]/N, N\cap F=\{0\}, N\neq(0).$$

根据定理 20,$N=(f(x)), f(x)$ 的首项系数为 1, 由 $N\neq(0)$ 且 $N\cap F=\{0\}, f(x)$ 为一个次数 ≥ 1 的多项式，$f(x)$ 由元素 u 唯一决定, 叫做元素 u 在 F 上的 **极小多项式**. 根据 $N=(f(x))$ 的定义可知一个代数元 u 的极小多项式 $f(x)$ 有如下的性质:

设 $f(x)$ 为域 F 上一个代数元 u 的极小多项式, 对 $g(x)\in F[x], g(u)=0 \iff f(x)|g(x)$.

定理 21 设 F 为一域，$F[x]$ 为 F 上一元多项式环，$f(x)\in F[x]$ 为一个次数 ≥ 1 的多项式，则下列叙述等价:

1) $f(x)$ 不可约，即 $f(x)$ 不能分解为两个次数较低的多项式的乘积.

2) 理想 $(f(x))$ 为极大.

3) $F[x]/(f(x))$ 为一域.

4) $F[x]/(f(x))$ 为一整环.

5) $(f(x))$ 为素理想.

证明 1)⇒2). 设 N 为 $F[x]$ 的任一理想使得 $(f(x))\subset N\subset F[x]$, 根据定理 20,$N=(g(x))$, 于是由 $(f(x))\subset(g(x))$ 有 $g(x)|f(x), f(x)=h(x)g(x)$, 因 $f(x)$ 不可约，$g(x)\sim f(x)$ 或 $g(x)\sim 1$(这里 "∼" 表示互相整除 (参见第四章 §1)). 即 $N=(f(x))$ 或 $N=(1)$, 所以 $(f(x))$ 为极大.

2)⇒3) 根据定理 7 即得.

3)⇒4) 显然.

4)⇒5) 根据定理 8 即得.

5)⇒1). 反证法. 假若 $f(x)$ 可约, 设 $f(x)=g(x)\cdot h(x), \deg g(x)<\deg f(x)$, $\deg h(x)<\deg f(x)$. 于是 $g(x)\notin(f(x)), h(x)\notin(f(x))$, 但是 $g(x)\cdot h(x)=f(x)\in(f(x))$. 这与 $(f(x))$ 为素理想矛盾. □

推论 1 设 S 为域 F 的一个扩环 (交换) 而且有相同的单位元素, 设 $u\in S$ 为 F 上的一个代数元, 则下列叙述等价:

1) u 在 F 上的极小多项式不可约.

2) $F[u]$ 为一域.

3) $F[u]$ 为一整环.

证明 由定理 14 的推论和定理 20 得 $F[u]\cong F[x]/(f(x))$. $f(x)$ 为 u 的极小多项式, 于是由定理 21 即得推论 1. □

推论 2 设 S 为一整环而且包含一个子域 F. 如果 S 的每个元素都是 F 上的代数元, 则 S 为一域.

证明 由推论 1 即得. □

最后应用上面几节的结果来说明一个有限域是如何产生的. 由第一章 §12, 知道任一个域有一个特征, 而且一个有限域的特征只能是一个素数. 设 F 为一个有限域, 特征为素数 p. 于是 F 的单位元素 e 的倍数 $e,2e,\cdots,pe=0$ 集合作成 F 的一个子域, 记作 $\mathbf{F}_p$, 即是特征 p 的素域. $\mathbf{F}_p$ 和整数环模 p 得到的商环 $\mathbf{Z}/(p)$ 同构. 其次, 根据定理 19 的推论, F 的非零元素全体 F^* 构成一个循环乘法群, 因而 F^* 有生成元. 设 α 是 F^* 的一个生成元. 设 $\mathbf{F}_p[x]$ 为 $\mathbf{F}_p$ 上一元多项式环. 根据定理 14 的推论, 存在一个环同态 $\sigma:\mathbf{F}_p[x]\to F$ 使得 σ 在 $\mathbf{F}_p$ 上为恒等映射而且 $\sigma(x)=\alpha$,σ 显然是满的. 令 $\ker(\sigma)=I$. 根据定理 20,I 是一个主理想, $I=(f(x))$. 于是

$$\mathbf{F}_p[x]/(f(x))\cong F.$$

根据定理 21 的推论 1,$f(x)$ 是一个不可约多项式. 设 $\deg f(x)=n$. 令 $\overline{x}=x+I$, 对于 $a\in\mathbf{F}_p$,$a+I$ 简记作 a(因为 $I\cap\mathbf{F}_p=(0)$), 于是 $\mathbf{F}_p[x]/(f(x))$ 的元素可以唯一地写成

$$a_0+a_1\overline{x}+\cdots+a_{n-1}\overline{x}^{n-1},\quad a_i\in\mathbf{F}_p.$$

这表明 $\mathbf{F}_p[x]/(f(x))$ 和 F 的元素个数同是 p^n. 由此可知 p^n 个元素的有限域是否存在和素域 $\mathbf{F}_p$ 上 n 次不可约多项式是否存在, 这两个问题实质上是同一个问题. 在习题中将要让读者证明, 对于每个特征 p(p 为素数) 的素域 $\mathbf{F}_p$ 和每个正整数 n, 在 $\mathbf{F}_p[x]$ 中恒存在 n 次的不可约多项式, 而且还可以计算出其个数.

再举一个例子. 设 F 为一域, $M_n(F)$ 为 F 上 $n\times n$ 全矩阵环. $M_n(F)$ 系由全部 $n\times n$ 矩阵 $A=(a_{ij})_{n\times n}$ 组成, 其中 $a_{ij}\in F$. 在 $M_n(F)$ 中取定一个

矩阵 $A=(a_{ij})_{n\times n}$. A 与每个纯量矩阵 aE 乘法交换，这里 $a\in F$, E 为单位矩阵. 因此 A 在 F 上的全部多项式

$$a_0E+a_1A+\cdots+a_rA^r,\ a_i\in F, r\geq 0$$

组成 $M_n(F)$ 的一个子环，记作 $F[A]$. 将 F 的元素 a 与纯量矩阵 aE 等同，则 F 可以看成 $F[A]$ 的一个子域. $F[A]$ 就是 A 在 F 上生成的交换环. A 在 F 上是代数的，因为 $E, A, A^2,\cdots,A^{n^2}$ 在 F 上是线性相关的. 设 $f(x)\in F[x]$ 为 A 的极小多项式. 则 $f(x)$ 的次数 $\leq n^2$.(实际上 $\deg f(x)\leq n$, 这是高等代数中已知的结果) 由于 $M_n(F)$ 当 $n>1$ 时有零因子，$F[A]$ 当 $n>1$ 时一般不是整环. 因此 $f(x)$ 通常是可约的. 若 $f(x)$ 不可约，则 $F[A]$ 为一域. 以 $F=\mathbf{Q}$ 有理数域，$n=2$ 为例. 此时

$$A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

设 A 不是纯量矩阵，则 A 的极小多项式 $f(x)=x^2-(a+d)x+|A|$. $\mathbf{Q}[A]$ 的元素一般可写成 $gA+h, g, h\in\mathbf{Q}$. 分三种情况：

1) $f(x)$ 不可约. $\mathbf{Q}[A]$ 是一个二次域，即 $\mathbf{Q}[A]$ 作为 $\mathbf{Q}$ 上的线性空间是二维的.

2) $f(x)$ 可约而且无重根. 设 $f(x)=(x-x_1)(x-x_2)$ 而且 $x_1\neq x_2$, 令 $B=\dfrac{1}{x_2-x_1}\cdot(A-x_1E), C=\dfrac{-1}{x_2-x_1}\cdot(A-x_2E)$. 则 $B+C=E$ 而且 $B\cdot C=0$. 于是 $B^2=B, C^2=C$. 因 A 不是纯量矩阵，$B\neq 0, C\neq 0$. B 和 C 分别生成两个理想 $\mathbf{Q}B$ 和 $\mathbf{Q}C$. $F[A]$ 是它们的直和 $F[A]=\mathbf{Q}B\oplus\mathbf{Q}C$. $\mathbf{Q}B$ 和 $\mathbf{Q}C$ 都和 $\mathbf{Q}$ 同构.

3) $f(x)$ 可约但有重根. 可设 $f(x)=(x-x_1)^2$. 令 $B=A-x_1E_1$, 则 $B^2=0$. 由于 A 不是纯量矩阵，$B\neq 0$. B 是一个幂零矩阵. $\mathbf{Q}[A]$ 除它本身和零理想外，只有唯一的非平凡理想 $\mathbf{Q}B$, 而且是一个幂零理想，即 $(\mathbf{Q}B)^2=(0)$.

如果一个环 R 的理想 N 的若干次幂等于 (0), 则 N 叫做一个 **幂零理想**.

§8 多项式函数

数学分析和复变函数中所讨论的函数分别是实变量函数和复变量函数. 由于实数域和复数域有很好的拓扑结构，可以引进极限、连续等概念来研究函数. 这一节是讨论任意域 F 上的函数，函数的自变量只能在 F 内取值. 由于一般域没有好的拓扑结构，只能应用域的代数性质来研究函数，因此目前只限于研究多项式函数.

设 F 为任一域. F 作为集合, 每个映射 $f: F\to F$ 叫做 F 上的一个**函数**. 用 s 表示自变量, f 也记作 $f(s)$. $f(s)$ 在 $s=a$ 的值记作 $f(a)$. F 上的函数全体记成 F^F. 如通常的函数的加法和乘法, 在 F^F 内引进函数的加法和乘法. 设 f 和 g 为 F 上任意两个函数, 定义 $f+g$ 和 $f\cdot g$ 如下:

$$(f+g)(s)=f(s)+g(s),$$
$$(f\cdot g)(s)=f(s)\cdot g(s).$$

容易验证, F^F 对加法和乘法形成一个交换环.

F 的每个元素 a 规定一个常数函数 f_a

$$f_a(s)=a, \text{ 对所有的 } s\in F.$$

容易看出, f_0 是 F^F 的零元素, f_1 是 F^F 的单位元素. 而且有

$$f_a+f_b=f_{a+b}, \quad f_a\cdot f_b=f_{a\cdot b}.$$

由此可知映射 $a\mapsto f_a$ 是 F 到 F^F 的一个单一同态. 因此可将 a 与 f_a 等同使得 F 成为 F^F 的一个子域. 以后 F 的元素 a 表示常数函数 $a(s)=a$, 其中 s 为 F 的任一元素. 不难验证, F^F 是 F 上的一个线性空间.

在数学分析中除常数函数外最简单的函数就是对角线映射, 即自变量函数 x. 在这里的对角线映射即自变量函数就是 s. s 一方面是自变量, 同时也是函数. s 是这样一个函数, 它的函数值和对应的自变量的值处处相等. 我们要讨论的对象就是函数 s 在 F 上生成的子环 $F[s]$. $F[s]$ 的每个元素可表成

$$a_0+a_1s+\cdots+a_ns^n, \quad a_i\in F, n\geq 0.$$

它叫做 F 上的**多项式函数**.

设 $F[x]$ 为 F 上的一元多项式环. 根据定理 14 的推论, $F[x]$ 到 $F[s]$ 有一个同态 σ 使得 σ 在 F 为恒等映射而且 $\sigma(x)=s$. 设 $\ker(\sigma)=I$. 则有

$$F[x]/I\cong F[s], \quad I\cap F=\{0\}.$$

定理 22 设 F 为一域, F^F 为 F 到 F 的函数环, $F\subset F^F$ 为常数函数子域. s 为自变量函数, 即对所有 $a\in F$, $s(a)=a$. 于是

1) 当 F 为一个无限域时, $F[s]\cong F[x]$, s 在 F 上为超越的.

2) 当 F 为 q 个元素的有限域时, $F[s]\cong F[x]/I, I=(x^q-x)$, 即 s 在 F 上为代数的而且 s 的极小多项式为 x^q-x. 此时 $F^F=F[s]$, 即 F 到 F 的函数都是多项式函数.

证明 1) 设 $f(x) \in I$, 于是 $f(s)=0$, 即 $f(s)$ 为 F^F 中的零函数，也就是对所有 $a \in F$, $f(a)=0$. 因为 F 包含无限多个元素，根据定理 18, $f(x)=0$, 即 $I=(0)$. 所以 $F[s] \cong F[x]$, s 在 F 上为超越.

2) $g(x)=\prod_{\alpha\in F}(x-\alpha) \in F[x]$ 是一个 q 次多项式而且恰有 q 个不同的根. 另一方面，根据定理 19 的推论下面的说明，F 的元素全是 x^q-x 的根. 于是 $g(x)|(x^q-x)$. 而且它们的首项相同，所以 $g(x)=x^q-x$. 设 $f(x)\in I$, 则 $f(s)=0$, 即 F 的元素全是 $f(x)$ 的根. 于是 $g(x)|f(x)$, 即 $I\subset(g(x))$. 反之，显然 $(g(x))\subset I$, 所以 $I=(g(x))=(x^q-x)$, 因而 s 在 F 上是代数的，而且 x^q-x 为它的极小多项式. $F[s]$ 包含 q^q 个多项式函数

$$a_0+a_1s+\cdots+a_{q-1}s^{q-1},\quad a_i\in F.$$

所以 $|F[s]|=|F^F|$, $F[s]=F^F$. □

其次讨论多元多项式函数. 设 $S=F^{(n)}=F\times F\times\cdots\times F=\{(a_1,a_2,\cdots,a_n)\,|\,a_i\in F\}$. S 到 F 的映射全体按通常的函数加法和乘法成一环，记作 F^S. 在函数环 F^S 中有 n 个自变量函数 s_i, $i=1,\cdots,n$, 定义如下:

$$s_i((a_1,\cdots,a_n))=a_i.$$

这 n 个自变量函数 s_i 在 F 上生成 F^S 的一个子环 $F[s_1,\cdots,s_n]$, 它系由 $s_1,\cdots,s_n$ 的多项式

$$\sum_{i_1,\cdots,i_n} a_{i_1\cdots i_n}s_1^{i_1}s_2^{i_2}\cdots s_n^{i_n}$$

所组成，其中 $a_{i_1\cdots i_n}\in F$. 上述函数简记作 $f(s_1,\cdots,s_n)$. $f(s_1,\cdots,s_n)$ 在 $(a_1,\cdots,a_n)$ 的函数值为

$$f(s_1,\cdots,s_n)((a_1,\cdots,a_n))=\sum_{i_1,\cdots,i_n}a_{i_1\cdots i_n}a_1^{i_1}a_2^{i_2}\cdots a_n^{i_n}.$$

根据定理 15 的推论 1, 存在 F 上多元多项式环 $F[x_1,\cdots,x_n]$ 到 $F[s_1,\cdots,s_n]$ 的一个同态 σ 使得 σ 在 F 上为恒等映射而且 $\sigma(x_i)=s_i$. 设 $\ker(\sigma)=I$. 则

$$F[x_1,\cdots,x_n]/I\cong F[s_1,\cdots,s_n],\quad I\cap F=\{0\}.$$

定理 23 设 F 为一域. $S=F\times F\times\cdots\times F=F^{(n)}$. 又设 $s_1,\cdots,s_n$ 为函数环 F^S 中 n 个自变量函数: $s_i((a_1,\cdots,a_n))=a_i$, 对所有 $(a_1,\cdots,a_n)\in F^{(n)}$. 于是

1) 当 F 为无限域时，$F[x_1,\cdots,x_n]\cong F[s_1,\cdots,s_n]$, $s_1,\cdots,s_n$ 在 F 上代数无关；

2) 当 F 为 q 个元素的有限域时，

$$F[s_1,\cdots,s_n]\cong F[x_1,\cdots,x_n]/I,$$

I 为 $F[x_1,\cdots,x_n]$ 中由 $x_1^q-x_1,\cdots,x_n^q-x_n$ 生成的理想. 此时 $F^{F^{(n)}}=F[s_1,\cdots,s_n]$.

证明 1) 设 $f(x_1,\cdots,x_n)\in I$, 求证 $f(x_1,\cdots,x_n)=0$. 对 n 作归纳法. 当 $n=1$ 时，1) 即定理 22 中的 1). 假设定理中的 1) 对 $n-1$ 成立. 将 $f(x_1,\cdots,x_n)$ 表成

$$f(x_1,\cdots,x_n)=\sum_{i=0}^{m}f_i(x_1,\cdots,x_{n-1})x_n^i,$$

于是对于 $(a_1,\cdots,a_n)\in F^{(n)}$, 恒有

$$\begin{aligned}&f(s_1,\cdots,s_n)((a_1,\cdots,a_n))\\&=\sum_{i=0}^{m}f_i(a_1,\cdots,a_{n-1})a_n^i\equiv 0.\end{aligned}$$

令 $a_1,\cdots,a_{n-1}$ 任意取定，而让 a_n 取遍 F 的元素，由于 F 无限，根据定理 22 的 1), 推出

$$f_i(a_1,\cdots,a_{n-1})=0,\quad i=0,\cdots,m.$$

这 $m+1$ 个等式对所有 $(a_1,\cdots,a_{n-1})\in F^{(n-1)}$ 都成立. 即得

$$f_i(s_1,\cdots,s_{n-1})=0,\quad i=0,1,\cdots,m.$$

由归纳法假设可知 $f_i(x_1,\cdots,x_{n-1})=0\ (i=0,1,\cdots,m)$. 因而 $f(x_1,\cdots,x_n)=0$, 所以 $I=(0)$. 得

$$F[s_1,\cdots,s_n]\cong F[x_1,\cdots,x_n].$$

因而 $s_1,\cdots,s_n$ 在 F 上代数无关.

2) 由 $x_1^q-x_1,\cdots,x_n^q-x_n$ 在 $F[x_1,\cdots,x_n]$ 中生成的理想记作 I'. 求证 $I'=I$. 根据定理 22 的 2) 知 $I'\subset I$. 求证 $I\subset I'$. 先证明一个事实：任一 $f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$ 恒可表成

$$f(x_1,\cdots,x_n)=\sum_{i=1}^{n}q_i(x_1,\cdots,x_n)(x_i^q-x_i)+r(x_1,\cdots,x_n)\tag{1}$$

使得 $r(x_1,\cdots,x_n)$ 作为每个 x_i 的多项式，其次数都小于 q. 显然只需证明当 $f(x_1,\cdots,x_n)$ 为单项式 $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ 的情况上述事实成立即可. 由于 $x_j^q-x_j\in I'$,

即 $x_j^q \equiv x_j \pmod{I'}$, 因而每个 $x_j^{i_j} \equiv x_j^{r_j} \pmod{I'}$ 使得 $0 \le r_j < q$. 于是

$$x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n} \equiv x_1^{r_1}x_2^{r_2}\cdots x_n^{r_n} \pmod{I'},$$

其中 $0 \le r_j < q$, $j = 1, \cdots, n$. 这表明它可表成

$$x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n} = x_1^{r_1}x_2^{r_2}\cdots x_n^{r_n} + g(x_1, \cdots, x_n),$$

其中 $g(x_1, \cdots, x_n) \in I'$. 因而任一 $f(x_1, \cdots, x_n)$ 可表成 (1) 式. 现在假设 $f(x_1, \cdots, x_n) \in I$. 由于 $I' \subset I$, (1) 式的左边和右边第一项都属于 I, 因而 $r(x_1, \cdots, x_n) \in I$. 由于 $r(x_1, \cdots, x_n)$ 对每个 x_j 的次数都小于 $|F| = q$, 仿 1) 的证明, 对 n 作归纳法可证 $r(x_1, \cdots, x_n) = 0$. 因而 $f(x_1, \cdots, x_n) \in I'$. 所以 $I \subset I'$. 总之 $I = I'$.

同时也证明了, 所有单项式 $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$, $0 \le i_1, \cdots, i_n < q$, 在 F 上的一切线性组合构成 $F[x_1, \cdots, x_n]$ 模 I 的一个完全剩余代表系, 即关于理想 I 的陪集代表. 所以 $F[x_1, \cdots, x_n]/I$ 的元素个数为 q^{q^n}, 它等于函数环 $F^{F^{(n)}}$ 的元素的个数. 因此得 $F[s_1, \cdots, s_n] = F^{F^{(n)}}$. □

根据以上讨论, 将 F 上一个多元多项式 $f(x_1, \cdots, x_n)$ 作为函数理解时, 若 F 无限, 则它们在同构意义下没有区别; 若 F 有限, 则 $f(x_1, \cdots, x_n)$ 作为函数理解时, 对应于它所代表的关于理想 $(x_1^q - x_1, \cdots, x_n^q - x_n)$ 的陪集 (其中 $q = |F|$), 而且这种对应是一一的.

习 题

(下列各题中出现的环, 除相反的声明外, 都假定是有单位元素的环)

1. 证明, 在环 R 内, 若 $1 - ab$ 有逆, 则 $1 - ba$ 也有逆.

2. 设在环 R 中元素 u 有右逆, 证明下列三条等价:

(i) u 有多于一个的右逆;

(ii) u 是一个左零因子;

(iii) u 不是单位.

3. 在环 R 内, 若元素 u 有多于一个的右逆, 则它有无穷多个右逆.

4. 已知一个交换环 R 的全部幂零元构成 R 的一个理想. 在非交换环内, 上述事实是否成立?

5. 设 F 为一个特征 p 的域, p 为素数, 证明

$$(a+b)^p = a^p + b^p, \quad 对所有\ a, b \in F.$$

域的特征概念可以推广到幺环上去. 如果幺环 R 的单位元素 e 生成的加法群 $G = \{ne \mid n \in \mathbf{Z}\}$ 是一个无限群, 则 R 叫做特征 0 的环; 若 G 是一个有限群, 令 $k = |G|$, 则 k

叫做环 R 的特征. 证明, 若 R 为整环, 则 R 的特征为 0 或为一个素数. 而且若 R 的特征为素数 p, 则上面等式对 R 也成立.

6. 设 $M_n(R)$ 为环 R 上 $n\times n$ 全矩阵环, 又设 I 为 R 的一个理想, 求证 I 上 $n\times n$ 全矩阵环 $M_n(I)$ 是 $M_n(R)$ 的理想. 进一步证明, $M_n(R)$ 除这一类理想外再无其它理想.

7. 设 I,H,N 为环 R 的理想. 证明

$$(H+N)\cdot I=H\cdot I+N\cdot I,\quad I\cdot(H+N)=I\cdot H+I\cdot N.$$

8. 设 $\eta:R\to R'$ 是一个满的环同态而且将 R 的单位元素 1 映到单位元素 $1'$. 指出下列命题的正确和错误. 正确的给以证明, 错误的请举反例.

(i) 若 $a\in R$ 是幂零 (幂等) 元, 则 $\eta(a)$ 也是 R' 的幂零 (幂等) 元 (如果环的元素 e 适合 $e^2=e$, 则 e 叫做 **幂等元**.)

(ii) 若 $a\in R$ 是零因子, 则 $\eta(a)$ 也是 R' 的零因子.

(iii) 若 R 为整环, 则 $\eta(R)=R'$ 也是整环.

(iv) 若 $\eta(R)=R'$ 为整环, 则 R 也是整环.

(v) 若 $u\in R$ 为单位, 则 $\eta(u)$ 也是 R' 的单位.

(vi) 若 $\eta(u)$ 是 R' 的单位, 则 u 也是 R 的单位.

9. 在四元数体 H 内, 令

$$H_0=\{a_0+a_1I+a_2J+a_3K\,|\,a_i\in\mathbf{Q}\}.$$

证明 H_0 是 H 的子体.

10. 决定四元数体 H 的中心.

11. 决定 H 中与 I 乘法交换的元素全体.

12. 设 S 是 H 的一个子体. 若对所有非零元素 $d\in H$ 都有 $dSd^{-1}\subset S$, 则 $S=H$ 或者 S 被包含在 H 的中心内.

13. 设 I,H,N 为环 R 的理想. 若 $H\cdot N\subset I$ 而且 I 与 H 互素, 则 $N\subset I$.

14. 设 I,H,N 是交换环 R 的理想. 若 $H\supset I, N\supset I$ 而且 H,N 互素, 则 $H\cdot N\supset I$.

15. 在域 F 上 $n\times n$ $(n>1)$ 全矩阵环 $M_n(F)$ 内寻求一个子环 R 使得 R 除恒等同构外没有其它反自同构.

16. 设 $R=\left\{\begin{pmatrix} a & 0\\ b & c\end{pmatrix}\middle|\, a,b\in\mathbf{Z}\right\}$. 试决定 R 的全部理想.

17. 试计算环 $R_n=\mathbf{Z}/(n)$ 上 2×2 全矩阵环的单位群的阶.

18. 设 R 为交换环 (不必有 1). 若 R 有零因子但又只有有限个零因子, 则 R 是一个有限环.

19. 设 N 为环 R(不必有 1) 的理想, 而且 I 又为 N(作为一个环) 的理想, 问 I 是不是 R 的理想?

20. 设 R 为一个交换环, a 是 R 的不可逆元. 证明 R 有一个极大理想 M 而且包含 a.

21. 设 R 为一交换环，$J(R)$ 表示 R 的全部极大理想的交. $J(R)$ 叫做环 R 的 **雅各布森** (Jacobson) **根**. 证明，$J(R)$ 的每个元素 a 有如下性质：对所有 $x \in R, 1-ax$ 都是可逆元. (与第二章定理 9 推论 2 第一章习题 38 作比较.)

22. 设 R 为一交换环. 如果元素 $a \in R$ 具有习题 21 中的性质，则 a 叫做一个 **强拟正则元**. 证明，R 的强拟正则元都属于 $J(R)$.(参看习题 21.)

23. 设 R 为一交换环. 证明，若 R 有限，则 R 的素理想都是极大理想.

24. 证明第三章 §2 的定理 4 和定理 $5'$ 等价.

25. 设 G 是复数域中全部单位根组成的乘法群. 请具体写出 G 的一个自同态，它是满的但不是单一的.

(以下 26 题至 29 题可参考华罗庚、万哲先著的《典型群》一书第一章 §4.)

26. 如果环 R 到环 R' 的映射 η 满足

(i) η 是加法群同态，即 $\eta(a+b)=\eta(a)+\eta(b)$;

(ii) $\eta(1)=1'$;

(iii) $\eta(aba)=\eta(a)\eta(b)\eta(a)$;

则 η 叫做一个 **若尔当** (Jordan) **同态**. 证明，若 η 是一个若尔当同态，则 η 具有性质

(i) $\eta(a^k)=\eta(a)^k$;

(ii) $\eta(abc+cba)=\eta(a)\eta(b)\eta(c)+\eta(c)\eta(b)\eta(a)$;

(iii) $\eta(ab+ba)=\eta(a)\eta(b)-\eta(b)\eta(a)$.

显然环的同态和反同态都是若尔当同态.

27. (雅各布森 - 瑞卡特 (Jacobson-Rickart)) 若 η 是环 R 到无零因子的环 R' 的一个若尔当同态，那么对任意 $a,b \in R$，$\eta(ab)=\eta(a)\eta(b)$ 和 $\eta(ab)=\eta(b)\eta(a)$ 有一成立.

28. (华罗庚) 设 η 为环 R 到环 R' 的一个映射，满足

(i) $\eta(a+b)=\eta(a)+\eta(b)$;

(ii) $\eta(1)=1'$;

(iii) $\eta(ab)=\eta(a)\eta(b)$ 或 $\eta(ab)=\eta(b)\eta(a)$, $a,b \in R$;

则 η 是一个同态或反同态. (后者定义为 R 到 R' 的映射 η 满足 (i),(ii) 和 (iii), $\eta(ab)=\eta(b)\eta(a)$.)

29. (雅各布森 - 瑞卡特) 证明，环 R 到无零因子的环 R' 的任一个若尔当同态是一个同态或反同态.

30. 设 p 为一素数，n 为任一大于 1 的整数，$R=\mathbf{Z}/(p^n)$. 证明

(i) R 的元素不是单位便是幂零元;

(ii) R 恰有一个素理想，记作 P;

(iii) 商环 R/P 是一个域.

31. 设 p 为一素数、n 为一整数，$R=\mathbf{Z}/(p^n)$, 试具体指出多项式环 $R[x]$ 中哪些元素是单位，零因子或是幂零元.

32. 设 $R=R_1\oplus R_2\oplus\cdots\oplus R_r$ 是环 R 的一个内直和，N 为 R 的一个理想. 证明

$$N=(N\cap R_1)\oplus(N\cap R_2)\oplus\cdots\oplus(N\cap R_r),$$

其中 $N\cap R_i$ 有可能等于 (0). 设 $n>1$, 试决定 $R=\mathbf{Z}/(n)$ 的最大幂零理想和单位群.

33. 证明 x^3-x 在 $\mathbf{Z}/(6)$ 内有 6 个根.

34. 证明 x^2+1 在四元数体 H 内有无穷多个根.

35. 在复数域内, $u=\sqrt{2}+\sqrt{3}$ 是有理数域 $\mathbf{Q}$ 上的代数元, 求 u 的极小多项式.

36. 在复数域内设 u 为 $f(x)=x^3-x+1$ 的一根, 试将下列元素

$$(5u^2+3u-1)(2u^2-2u+6) \text{ 和 } (3u^2-u+2)^{-1}$$

表成次数不超过 2 的 u 的多项式.

37. 设 $\mathbf{F}_2=\mathbf{Z}/(2)$. 证明 $f(x)=x^3+x^2+1$ 在 $\mathbf{F}_2[x]$ 内不可约, 并且证明商环 $R=\mathbf{F}_2[x]/(x^3+x^2+1)$ 是 8 个元素的域.

38. 设 $\mathbf{F}_5=\mathbf{Z}/(5)$. 试定出 $\mathbf{F}_5[x]$ 中全部首项系数为 1 的 2 次不可约多项式.

39. 造一个 25 个元素的域.

40. 证明 $\mathbf{Z}[x]$ 的理想 $(3, x^3+2x^2+2x-1)$ 不是主理想.

41. 设 $\mathbf{F}_3=\mathbf{Z}/(3)$. $I=(3,x^3+2x^2+2x-1)$ 为 $\mathbf{Z}[x]$ 的理想. 证明

$$\mathbf{Z}[x]/I\cong \mathbf{F}_3[x]/(x^3-x^2-x-1).$$

由此证明 I 为 $\mathbf{Z}[x]$ 的一个极大理想.

42. 设 F 为一域, $f(x)\in F[x]$, $\deg f(x)>0$. 证明商环 $F[x]/(f(x))$ 无幂零元的充要条件是 $f(x)$ 无重因式.

43. 设 R 为一个交换环. 若 $f(x)\in R[x]$ 是一个幂零元, 则 $f(x)$ 的每个系数也是 R 的幂零元.

44. 设 R 为一交换环. 证明, 若 $f(x)\in R[x]$ 是一个零因子, 则存在 R 的一个元素 a, $a\neq 0$ 使得 $af(x)=0$. 反之显然.

45. 设 R 为一交换环, $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n\in R[x]$. 若 a_n 为单位而 $a_0,\cdots,a_{n-1}$ 为幂零元, 则 $f(x)$ 为 $R[x]$ 的单位.

46. 证明习题 43 的逆也成立.

47. 设 R 为交换环, $R'=R[x_1,\cdots,x_n]$. 用 $r(R)$ 表示 R 的诣零根. 证明 R' 的诣零根 $r(R')$ 等于 $r(R)[x_1,\cdots,x_n]$.

48. 在一个有限环 R 中, 若一个元素有右逆, 则它必有左逆. 因而它有逆. 当 R 无限时, 这个事实对不对?

49. 设 R 为一交换环, 证明, 多项式环 $R[x]$ 的强拟正则元都是幂零元.

50. 设 R 为一交换环. 证明, 若 R 的每个元素 a 都有一个适当方幂 $a^n=a$ $(n>1)$, 则 R 的每个素理想都是极大理想.

51. 如果一个交换环 R 的每个元素 a 满足 $a^2=a$, 则 R 叫做一个布尔 (Boole) 环. 证明布尔环 R 有性质:

(i) $2a=0$. 对所有 $a\in R$;

(ii) 每个素理想 I 都极大而且 R/I 是特征 2 的素域;

(iii) R 的每个有限生成的理想都可由一个元素生成.

52. 设 R 为一交换环，$r(R)$ 为它的诣零根. 证明下列三条等价:

(i) R 有一个而且只有一个素理想;

(ii) R 的每个元素不是单位便是幂零元;

(iii) $R/r(R)$ 是一个域.

53. 求证，如果一个整环只有有限多个理想，则它是一个域.

54. 设 R 为一整环. 求证，如果 R 的任一由理想组成的非空集合按包含关系都有一个极小元，则 R 为一域.

55. (华罗庚) 设 a,b 为一环 R 的两个单位，而且 $ab-1$ 也是单位. 求证 $a-b^{-1}$ 和 $(a-b^{-1})^{-1}-a^{-1}$ 也是单位，而且满足下列恒等式

$$((a-b^{-1})^{-1}-a^{-1})^{-1}=aba-a.$$

(此题如在第一章已经作过，则可直接应用于下题.)

56. (嘉当 - 布饶尔 - 华 (Cartan-Brauer-Hua)) 设 D 为一体，C 为它的中心即 $C=\{x\in D\,|\,xy=yx$ 对所有 $y\in D\}$. 又设 R 为 D 的一个子体. 证明，如果 $dRd^{-1}\subset R$ 对 D 的所有非零元成立，则 $R=D$ 或者 $R\subset C$. (参见华罗庚、万哲先著的《典型群》第一章 §10.)

57. 令 R 表示实系数多项式函数全体. 按函数的加法和乘法，R 成一环. 证明

(i) 对每个实数 t, 映射 $\eta_t: f(x)\mapsto f(t)$, $f(x)\in R$, 是 R 到实数域 $\mathbf{R}$ 的一个环同态;

(ii) R 到 $\mathbf{R}$ 的任一个环同态必是某一个 η_t.

58. 设 F 为一个无限域，在多项式环 $F[x_1,\cdots,x_n]$ 中任给两个多项式 $f(x_1,\cdots,x_n)$ 和 $g(x_1,\cdots,x_n)$ 而且 $g(x_1,\cdots,x_n)\neq 0$. 证明，如果使 $g(c_1,\cdots,c_n)\neq 0$ 的所有点 $(c_1,\cdots,c_n)$ 而有 $f(c_1,\cdots,c_n)=0$, 则 $f(x_1,\cdots,x_n)=0$.

59. 设 F 为 q 个元素的有限域 (注意 F 的每个非零元素 a 有 $a^{q-1}=1$). 在多项式环 $R=F[x_1,\cdots,x_n]$ 中，多项式 $g_0(x_1,\cdots,x_n)=(1-x_1^{q-1})(1-x_2^{q-1})\cdots(1-x_n^{q-1})$ 具有如下性质:

$$g_0(a_1,\cdots,a_n)=\begin{cases}1, & 当\ (a_1,\cdots,a_n)=(0,\cdots,0),\\ 0, & 当\ (a_1,\cdots,a_n)\neq(0,\cdots,0).\end{cases}\tag{1}$$

60. F,R 假设如习题 59. 若多项式 $f(x_1,\cdots,x_n)\in R$ 具有性质

$$f(a_1,\cdots,a_n)=\begin{cases}0, & 当\ (a_1,\cdots,a_n)=(0,\cdots,0),\\ 非零元, & 当\ (a_1,\cdots,a_n)\neq(0,\cdots,0).\end{cases}$$

则 $g(x_1,\cdots,x_n)=1-f(x_1,\cdots,x_n)^{q-1}$ 如同 $g_0(x_1,\cdots,x_n)$ 一样具有性质 (1). 由此进一步证明 $g(x_1,\cdots,x_n)$ 的次数 $\geq n(q-1)$.

61. (阿廷 - 谢瓦莱 (Artin-Chevalley)) 设 F,R 如习题 59. 设 R 中多项式 $f(x_1,\cdots,x_n)$ 的次数 $r<n$, n 为未定元 x_i 的个数，而且假定 $f(0,\cdots,0)=0$. 证明 $f(x_1,\cdots,x_n)$ 除 $(0,\cdots,0)$ 外还有另一个零点，即存在一个 $(a_1,\cdots,a_n)\neq(0,\cdots,0)$ 使得 $f(a_1,\cdots,a_n)=0$.

62. 设 R 为交换环. $(a_i)=(a_0,a_1,a_2,\cdots)\in R[[x]]$, $a_i\in R$. 令 $x=(0,1,0,0,\cdots)$. (a_i) 可写成 $f=\sum\limits_{i=0}^{\infty}a_ix^i$. 证明:

(i) f 是 $R[[x]]$ 的单位当且仅当 a_0 是 R 的单位;

(ii) $R[[x]]$ 为整环当且仅当 R 为整环;

(iii) 设 R 为整环. $R[[x]]$ 的商域记成 $F\{x\}$, 其中 F 为 R 的商域. $F\{x\}$ 的元素 g 可写成

$$g = x^{\nu}(a_0 + a_1x + a_2x^2 + \cdots), \quad a_i \in F, a_0 \neq 0, \nu \in \mathbf{Z}.$$

63. 证明, 如果在交换环 R 中每个非单位 a 与 1 的和 $1+a$ 为单位, 则 R 的全部非单位构成 R 的一个极大理想, 而且是 R 的唯一极大理想. 这种环是否存在?

64. 证明: 如果在整环 R 中每个非单位 a (0 除外) 与 1 的和 $1+a$ 仍为非单位, 于是

(i) R 的全部单位加上 0 构成 R 的一个子域, 记作 F;

(ii) R 中 F 以外的元素都是 F 上的超越元.

65. 证明. 若 F 为一无限域, 则不存在非零多项式 $f(x) \in F[x]$ 使得 $f(x) \cdot f(y) = f(x+y)$, 其中 x, y 在 F 上代数无关.

66. 设 F 为一域, $M_n(F)$ 为 F 上全矩阵环. 证明: $M_n(F)$ 的每个左理想都是主理想.

67. 设 G 为一个阿贝尔群, η 与 ξ 为 G 的自同态. 我们定义 η 与 ξ 的积 $\eta \cdot \xi$ 为

$$\eta \cdot \xi(a) = \eta(\xi(a)), \quad a \in G.$$

显然 G 的自同态全体 $\mathrm{End}(G)$ 形成一个乘法幺半群. 由于 G 的运算交换, 我们还可以定义 η 与 ξ 的和 $\eta + \xi$ 为

$$(\eta + \xi)(a) = \eta(a) + \xi(a), \quad a \in G.$$

验证 $\eta + \xi$ 是 G 的一个自同态. 显然 $\mathrm{End}(G)$ 构成一个环, 有单位元素, 叫做交换群 G 的 **自同态环**.

68. 试决定下列阿贝尔群的自同态环:

(i) 整数加法群 $\mathbf{Z}_+$;

(ii) n 阶循环群 $G = \langle \sigma \rangle$;

(iii) 有理数加法群 $\mathbf{Q}_+$;

(iv) p^n 阶的初等 p- 群 $(p, p, \cdots, p)$.

第四章　整环的整除性

这一章我们着手建立整环上的整除性理论. 回顾一下, 我们已经在整数环上和域上一元多项式环上建立了整除的理论. 这两个环有许多共同之处, 它们都有除法算式, 最大公因子的概念, 最后得到唯一因子分解定理. 前一节还证明了它们都是主理想整环, 能够保持这两种环的共同特征而又更一般一些的环有欧几里得整环和主理想整环. 下面先来讨论主理想整环. 为此首先明确整环上的整除概念.

§1　主理想整环

设 R 为一整环. 对任意元素 $a, b \in R$, 如果存在一个元素 $c \in R$ 使得 $a = bc$, 则 b 叫做 a 的 **因子**,a 叫做 b 的 **倍数**,b 叫做 **整除**a, 记作 $b|a$. 整除具有反身性 $a|a$ 和传递性: $b|a$ 且 $c|b \Rightarrow c|a$. 还有性质: $c|a$ 且 $c|b \Rightarrow c|(ua+vb)$, $u, v \in R$. $1|a|0$ 对所有 $a \in R$ 成立.

1 的所有因子构成的集合 $U = \{u \in R \mid u|1\}$ 恰好就是 R 的单位全体构成的乘法群. 令 $Ua = \{ua \mid u \in U\}$.

如果 $a|b$ 同时 $b|a$, 则 a, b 叫做 **相伴**. 相伴显然具有对称性, 和整除一样有反身性和传递性, 因而是一个等价关系. a, b 相伴记作 $a \sim b$. 若 $a \sim b$, 则 $b = ua$, 同时 $a = vb$, 因而 $a = vua$, 除去 $a = 0$ 外, $uv = 1$, 因而 $u, v \in U$. 反之, 若 $a = vb$, $v \in U$, 则 $b = v^{-1}a$, a, b 相伴. 因此与 a 相伴的元素全体为 Ua. 最后相伴还有乘法同余关系, 即若 $a \sim b, c \sim d$, 则 $ac \sim bd$.

若 $b|a$ 但 $a \nmid b$, 则 b 叫做 a 的 **真因子**, 每个非零元 a 有两类平凡因子即 U 和 Ua.

设元素 a 不是单位, 不是零. 若从 $a = bc$ 恒推出 $b \sim a$ 或 $b \sim 1$, 则 a 叫做一个 **不可约元**. 一个不可约元 a 除两类因子 U 和 Ua 外无其它因子. 设元素 a 不是 0 不是单位. 若从 $a|bc$ 恒推出 $a|b$ 或 $a|c$, 则 a 叫做一个 **素元**.

整数环 $\mathbf{Z}$ 的单位群为 $\{\pm 1\}$, 素数是不可约元, 也是素元. 域上一元多项式环 $F[x]$ 的单位群是 $F^* = F - \{0\}$, 不可约多项式就是不可约元, 同时也是素元.

若 $c|a$ 且 $c|b$, 则 c 叫做 a, b 的一个 **公因子**. a, b 的一个公因子 d 叫做 a, b 的一个 **最大公因子**, 如果 $c|a$ 且 $c|b$ 则必有 $c|d$. 任意 a, b 的最大公因子不一定存在, 如果 a, b 的最大公因子存在, 则 a, b 的任意两个最大公因子 d_1, d_2 根据定义它们互相整除, 因而相伴 $d_1 \sim d_2$.

引理 1 设 R 为一个整环, a, b 为 R 的任意元素, 于是

1) $a|b \iff (b) \subset (a)$. 因而 $a \sim b \iff (a) = (b)$. 而且若 $a|b$ 但 $a \not\sim b$, 则 $(b) \subset (a)$ 但 $(b) \neq (a)$; 反之也对.

2) a 为素元 $\iff$ (a) 为非零素理想. 因此, 若 (a) 为非零极大理想, 则 a 为素元.

3) 素元是不可约元. 因此, 若 (a) 为非零素理想, 则 a 为不可约元.

证明 1) 若 $a|b$, 则 $b \in (a)$, 从而 $(b) \subset (a)$. 反之, 若 $(b) \subset (a)$ 则 $b \in (a)$, 从而 $ac = b, a|b$. 从此直接导出 $a \sim b \iff (a) = (b)$. 然后得到最后一个结果.

2) 根据素理想和素元的定义即得第一个结果. 若 (a) 为非零极大理想, 根据第三章 §4、定理 7 和 8 知 (a) 为非零素理想, 因而 a 为素元.

3) 设 a 为素元. 反证法. 假若 a 可以分解成两个真因子 b,c 的积 $a = bc$. 从而 $a|bc$. 由于 a 为素元, 于是 $a|b$ 或 $a|c$, 即 $a \sim b$ 或 $a \sim c$. 这与 b,c 是 a 的真因子矛盾. □

下面将要看到在一般整环中不可约元不一定是素元, 素理想不一定是极大理想. 但是在主理想整环中则有

引理 2 设 R 为一个主理想整环, 则有

1) 若 a 为不可约元, 则 (a) 为极大理想;

2) 不可约元为素元;

3) 每个非零素理想都是极大理想.

证明 1) 设 a 为不可约元. 设 N 为 R 的任一个理想使得 $(a) \subset N$ 但 $(a) \neq N$. 由于 R 是主理想整环, $N = (b)$. 从 $(a) \subset N$ 有 $b|a$. 但是 $(a) \neq N$, 因而 $b \not\sim a$. 所以 b 是 a 的一个真因子. 由于 a 不可约, 得 $b \sim 1$, 即 $N = (b) = R$. 所以 (a) 为 R 的极大理想.

2) 设 a 为不可约元, 则 (a) 为极大理想. 从而 (a) 也是素理想. 根据引理 1,a 为素元.

3) 设 N 为 R 的任一非零素理想. 由于 R 是主理想整环, $N = (a), a \neq 0$. 根据引理 1,a 为不可约元. 从而 (a) 为极大理想. □

引理 3 设 R 为一个主理想整环. 对于 $a, b \in R$, 若 $(a) + (b) = (d)$, 则 d 是 a,b 的一个最大公因子, 而且 d 可表成

$$d = ua + vb, \quad u, v \in R.$$

证明 由 $(a) \subset (d), (b) \subset (d)$ 得 $d|a, d|b$. d 为 a,b 的公因子. 设 $c|a, c|b$, 于是 $(a) \subset (c), (b) \subset (c)$, 从而 $(a) + (b) = (d) \subset (c)$, 于是 $c|d$. 所以 d 为 a,b 的一个最大公因子. □

多个元素 $a_1, \cdots, a_r$ 的最大公因子可以归纳地定义. 于是直接得到下列

推论 设 R 为一个主理想整环. 对于 $a_1,\cdots,a_r\in R$, 若 $(a_1)+\cdots+(a_r)=(d)$, 则 d 为 $a_1,\cdots,a_r$ 的一个最大公因子而且 d 可表成

$$d=u_1a_1+\cdots+u_ra_r,\quad u_i\in R,\ i=1,\cdots,r.\quad \square$$

如果环 R 的理想序列 $N_1,N_2,\cdots$ 满足条件

$$N_i\subset N_{i+1},\quad i=1,2,\cdots$$

则 $\{N_i\}$ 叫做一个 **理想升链**.

如果整环 R 的元素序列 $a_1,a_2,\cdots$, 满足条件

$$a_{i+1}|a_i,\quad i=1,2,\cdots$$

则 $\{a_i\}$ 叫做一个 **因子降链**.

对主理想整环 R 来说, R 的任一个理想升链 $\{(a_i)\}$ 可以转换成一个因子降链 $\{a_i\}$. 反之也对.

引理 4 1) 主理想整环 R 的任一个理想升链 $\{(a_i)\}$ 恒有限. 即存在一个正整数 m 使得 $(a_m)=(a_{m+1})=(a_{m+2})=\cdots$.

2) 对主理想整环 R 的任一因子降链 $\{a_i\}$, 恒存在一个正整数 m 使得 $a_m\sim a_{m+1}\sim a_{m+2}\sim\cdots$.

证明 根据引理 1, 1) 和 2) 等价. 现证明 1). 令 $N=\bigcup\limits_i(a_i)$. 首先证明 N 是一个理想. 对于 $a,b\in N$, 有 a,b 分别属于某个 (a_r) 和 (a_s). 不妨设 $r\leq s$, 于是 $(a_r)\subset(a_s)$. 从而 $a\in(a_s)$. $a-b\in(a_s)$. 因而 $a-b\in N$. 对于 $c\in R$, 由 $a\in(a_r)$ 得 $ac\in(a_r)$, 因而 $ac\in N$. 所以 N 是 R 的一个理想. 因为 R 是主理想整环, $N=(d)$. 根据 N 的定义, d 属于某个 (a_m). 从而 $N\subset(a_m)$. 反之, 显然 $(a_m)\subset N$. 所以 $N=(a_m)$. 对任意大于 m 的整数 n 有 $(a_m)\subset(a_n)\subset N$. 由 $(a_m)=N$ 推出 $(a_n)=N$. 最后得 $N=(a_m)=(a_{m+1})=(a_{m+2})=\cdots$. $\square$

综上所述, 主理想整环保留了整数环和域上一元多项式环的几乎一切整除性质 (除法算式除外). 而且从主理想整环的定义出发, 导出这些性质显得极其简明而自然. 因此在主理想整环上进一步建立唯一因子分解定理是很自然的事情. 这将在 §3 进行更广泛的讨论. 现在提两个问题. 其一是除上述两个例子外是否还有其它的主理想整环? 在 §5 末从整数环 $\mathbf{Z}$ 和每个素数 p 出发作出了无穷多个分式环 $S_p^{-1}\mathbf{Z}$, 其中 $S_p=\mathbf{Z}-(p)$. 它们都是主理想整环. 在下一节为我们提供了另一类主理想整环. 第二个问题是在主理想整环中如何有效地计算两个元素的最大公因子? 在整数环和域上一元多项式环中欧几里得除法就是一个

计算最大公因子的有效算法，但它是建立在除法算式上面的．而对任意的主理想整环来说，这种除法算式不存在．为了强调这一优点，我们将在下一节介绍一类特殊的主理想整环，即欧几里得整环．

最后让我们举一个非主理想整环的例子．

例 设 $\mathbf{Z}[x]$ 为整数环 $\mathbf{Z}$ 上一元多项式环．证明 $\mathbf{Z}[x]$ 是一个非主理想整环．我们来证明由 2 和 x^2+1 生成的理想 $(2,x^2+1)$ 不是主理想．假若它是主理想．可设 $(2,x^2+1)=(g(x))$．一方面，由 $2\in(g(x)), g(x)|2$．于是存在 $h(x)\in\mathbf{Z}[x]$ 使得 $2=g(x)h(x)$．由于 $\mathbf{Z}[x]$ 为整环，$\deg g(x)=0, \deg h(x)=0$，因而 $g(x)=1$ 或 2 (不妨取 $g(x)>0$)．另一方面，由 $(2,x^2+1)=(g(x))$，可知 $g(x)$ 可表成 $g(x)=u(x)(x^2+1)+2v(x), u(x),v(x)\in\mathbf{Z}[x]$．用 $x=1$ 代入得 $g(1)=2(u(1)+v(1))$，从而 $2|g(1)$．所以 $g(x)=2$．再由 $(2,x^2+1)=(2)$，有 $x^2+1\in(2)$，x^2+1 可写成 $x^2+1=2h(x), h(x)\in\mathbf{Z}[x]$．矛盾．

§2 欧几里得整环

定义 1 设 R 为一个整环．如果存在 R 的乘法半群 $R^*=R-\{0\}$ 到自然数系 $\mathbf{N}$ 的一个函数 $d(x)$，使得对于任一对元素 $a,b\in R, b\neq 0$，存在一对元素 q 和 r 满足

$$a=qb+r,$$

其中 $r=0$ 或 $r\neq 0$，但 $d(r)<d(b)$，则 R 叫做一个 **欧几里得整环**．

例 1 整数环 $\mathbf{Z}$ 是一个欧几里得整环，如果对每个非零整数 a 规定 $d(a)=|a|$．

例 2 域 F 上一元多项式环 $F[x]$ 是一个欧几里得整环，如果对每个非零多项式 $f(x)$ 规定

$$d(f(x))=1+\deg f(x).$$

定理 1 欧几里得整环都是主理想整环．

证明 设 R 为一个欧几里得整环，$d(x)$ 为它的如定义中的函数．设 N 为 R 的任一理想．若 N 为零理想，则它当然是主理想 $N=(0)$．设 $N\neq(0)$．在 N 中存在一个非零元素 b 使得 $d(b)$ 是最小的，即 $d(b)\leq d(x)$ 对所有非零 $x\in N$．对于 N 的任意元素 a，存在一对元素 $q,r\in R$ 使得

$$a=qb+r,$$

其中 $r=0$ 或 $r\neq 0$ 而有 $d(r)<d(b)$．由于 N 为理想，$r=a-qb\in N$．根据 b 的取法，$r=0$．于是 $a=qb$，即 $a\in(b)$．从而 $N\subset(b)$．显然 $(b)\subset N$．所以 $N=(b)$． □

欧几里得整环实际上是具有除法算式的主理想整环. 正如整数环, 在欧几里得整环中可以应用欧几里得除法来求两个元素的最大公因子. 请注意, 同一个欧几里得整环 R 可能有不同的函数 $d(x)$.(当然是满足定义 1 中条件的函数.)

下面将从另一个来源来提供一类欧几里得整环和主理想整环.

令 $\mathbf{Q}$ 表示有理数域, m 表示一个整数, 假定 $m \neq 0, 1$, 而且不含平方因子. 在复数域 $\mathbf{C}$ 中由所有 $r + s\sqrt{m}, r, s \in \mathbf{Q}$, 组成的子集记作 $\mathbf{Q}(\sqrt{m})$. $\mathbf{Q}(\sqrt{m})$ 对复数加、减、乘、除封闭, 因而构成复数域的一个子域, 它叫做有理数域 $\mathbf{Q}$ 上的一个 **二次数域**. 有理数域中有一个重要的子环即整数环 $\mathbf{Z}$. $\mathbf{Q}(\sqrt{m})$ 中也有一个重要的子环, 即代数整数环. 如果 $\mathbf{Q}(\sqrt{m})$ 的元素 α 在 $\mathbf{Q}$ 上的极小多项式 (即以 α 为根的首项系数为 1 的次数最低的有理系数多项式) 是一个整系数多项式, 则 α 叫做一个 **代数整数**. 有理数 α 的极小多项式为 $x - \alpha$. 因而有理数 α 为代数整数当而且仅当 α 是有理整数. 其次, 设 $\alpha = s + t\sqrt{m}$, $t \neq 0$. 则 α 的极小多项式为 $x^2 - (\alpha + \overline{\alpha})x + \alpha \cdot \overline{\alpha} = x^2 - 2sx + (s^2 - mt^2)$(这里 $\overline{\alpha} = s - t\sqrt{m}$. $\alpha\overline{\alpha}$ 称为 α 的 **范数**, 记为 $N(\alpha)$). 因而 α 为代数整数当而且仅当 $2s$ 和 $s^2 - mt^2$ 都为整数. 令 $2s = a, a \in \mathbf{Z}$. 又令 $2t = b$. 则 $s^2 - mt^2 = \frac{1}{4}(a^2 - mb^2)$. 由此可知, α 为代数整数当而且仅当 a, b 为整数而且 $a^2 - mb^2 \equiv 0 \pmod 4$. 由此不难证明, 当 $m \equiv 2$ 或 $3 \pmod 4$ 时, a, b 为偶数即 s, t 为整数; 当 $m \equiv 1 \pmod 4$ 时, a, b 同奇或同偶. 反之显然. 用 R_m 表示 $\mathbf{Q}(\sqrt{m})$ 中代数整数全体. 于是

当 $m \equiv 2$ 或 $3 \pmod 4$ 时, $R_m = \{a + b\sqrt{m} \mid a, b \in \mathbf{Z}\}$.

当 $m \equiv 1 \pmod 4$ 时, $R_m = \{\frac{1}{2}(a + b\sqrt{m}) \mid a, b \in \mathbf{Z}$ 且 a, b 同奇或同偶$\}$.

由简单验算知, R_m 是 $\mathbf{Q}(\sqrt{m})$ 的一个子环, 叫做 $\mathbf{Q}(\sqrt{m})$ 的 **代数整数环**. 关于 R_m 在什么情况是主理想环, 甚至是欧几里得整环, 至今已知的结果有:

(1) 关于虚二次数域 $\mathbf{Q}(\sqrt{m})$, 其代数整数环为主理想整环的只有 9 种, 即 $m = -1, -2, -3, -7, -11, -19, -43, -67, -163$. 其中前 5 种还是欧几里得整环, 而且函数 $d(\alpha)$ 取 α 的范数 $N(\alpha) = \alpha\overline{\alpha}$, 它满足定义 1 中条件, 即能给出除法算式, 而后 4 种则不是欧几里得整环. 即满足定义 1 的函数 $d(x)$ 不存在.

(2) 关于实二次数域 $\mathbf{Q}(\sqrt{m})$, 其代数整数环的范数函数 $d(\alpha) = |N(\alpha)|$ 满足定义中条件的只有 16 种, 即 $m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$.

至于实二次数域的代数整数环 R_m 有多少为主理想整环, 高斯 (Gauss) 曾猜想有无限多个实二次域, 它们的代数整数环为主理想整环. 但至今未能证实.

例 1 证明高斯整数环 $R_{-1} = \mathbf{Z}[\sqrt{-1}]$ 为欧几里得整环.

注意 $-1 \equiv 3 \pmod 4$. 取函数 $d(x) = N(x)$. 对于 $\alpha, \beta \in R_{-1}, \beta \neq 0$. 令 $\frac{\alpha}{\beta} = t + s\sqrt{-1}, t, s \in \mathbf{Q}$. 取整数 u, v 使得 $|t - u| \leq \frac{1}{2}, |s - v| \leq \frac{1}{2}$, 令

$q = u + v\sqrt{-1}, r_1 = (t-u) + (s-v)\cdot\sqrt{-1}$. 于是 $\dfrac{\alpha}{\beta} = q + r_1$ 得

$$\alpha = q\beta + r_1\beta.$$

由于 $\alpha, \beta, q \in R_{-1}$, 从而 $r_1\beta \in R_{-1}$. 由计算 $d(r_1) = N(r_1) = (t-u)^2 + (s-v)^2 \leq \dfrac{1}{4} + \dfrac{1}{4} < 1$. 因而 $d(r_1\beta) = N(r_1\beta) = N(r_1)N(\beta) < N(\beta) = d(\beta)$. 取 $r = r_1\beta$, 则算式 $\alpha = q\beta + r$ 满足定义 1 中的条件.

仿例 1, 可证当 $m = -2, 2, 3$ 时 R_m 为欧几里得整环. 再举一个 R_m, $m \equiv 1 \pmod 4$ 的例子.

例 2 证明 R_{-3} 为欧几里得整环.

注意 $-3 \equiv 1 \pmod 4$, $R_{-3} = \left\{\dfrac{1}{2}(a + b\sqrt{-3}) \mid a, b \in \mathbf{Z}, a, b\text{同奇或同偶}\right\}$. 取函数 $d(x) = N(x)$. 对 $\alpha, \beta \in R_{-3}$, $\beta \neq 0$. 令 $\dfrac{\alpha}{\beta} = t + s\sqrt{-3}, t, s \in \mathbf{Q}$. 首先取一个整数 v 使得 $|2s - v| \leq \dfrac{1}{2}$. 然后取一个整数 u 使得 $|2t - u| \leq 1$ 而且保持 u 与 v 同奇或同偶. 令 $q = \dfrac{1}{2}(u + v\sqrt{-3}), r_1 = \dfrac{1}{2}(2t - u + (2s - v)\sqrt{-3})$. 于是 $\dfrac{\alpha}{\beta} = q + r_1$, 得

$$\alpha = q\beta + r_1\beta.$$

由于 $\alpha, q, \beta \in R_{-3}$, 从而 $r_1\beta \in R_{-3}$. 由计算

$$d(r_1) = N(r_1) = \left(\frac{2t-u}{2}\right)^2 + 3\left(\frac{2s-v}{2}\right)^2 \leq \frac{1}{4} + \frac{3}{16} < 1.$$

因而, 令 $r = r_1\beta$, 有

$$d(r) = d(r_1\beta) = N(r_1\beta) = N(r_1)N(\beta) < N(\beta) = d(\beta).$$

所以算式 $\alpha = q\beta + r$ 满足定义 1 的条件.

仿例 2, 可证当 $m = -11, -7, 5, 13$ 时 R_m 为欧几里得整环.

§3 唯一因子分解整环

定义 2 设 R 为一整环. 如果 R 满足下列两条件, 则 R 叫做一个 **唯一因子分解整环**, 也叫 **高斯整环**.

1) R 的每个非零非单位的元素 a 恒可写成有限多个不可约元素的积

$$a = p_1 p_2 \cdots p_r.$$

2) 上述分解在相伴意义下是唯一的,即若元素 a 有两种分解 $a = p_1p_2\cdots p_r = q_1q_2\cdots q_s$, 则 $r = s$ 而且适当改换 q_i 的脚标可使

$$q_i \sim p_i, \quad i = 1, 2, \cdots, r.$$

例 整数环和域上一元多项式环都是唯一因子分解整环. 将会立刻看到, 主理想整环也是唯一因子分解整环.

如果对于整环 R 的任一因子降链

$$a_1, a_2, \cdots \quad a_{n+1}|a_n, \quad n = 1, 2, \cdots$$

恒存在一个正整数 m 使得

$$a_m \sim a_{m+1} \sim a_{m+2} \sim \cdots$$

则说整环 R 满足 **因子链条件**.

引理 1 若整环 R 满足因子链条件, 则定义 2 中的条件 1) 在 R 内成立.

证明 反证法. 假设条件 1) 在 R 内不成立. 用 S 表示 R 中不满足条件 1) 的非零非单位的元素构成的子集, 则 S 非空. 用 P 表示由 S 的一切非空子集作元素构成的集. 设 f 为 P 上的一个选择函数, 即 f 是一个映射 $P \to S$ 使得 $f(A) \in A$ 对所有 $A \in P$.(参看第零章 §7) 对于任一元素 $a \in S$, 用 $S(a)$ 表示 a 在 S 中的全部真因子构成的子集. 求证 $S(a)$ 对所有 $a \in S$ 都不是空集. 因为 $a \in S$, a 不是不可约元, 设 $a = bc$ 为一个 **真分解**, 即 b, c 都不是单位. 若 b 和 c 都不属于 S, 则 b 和 c 都可以写成有限多个不可约元的乘积, 那么 $a = bc$ 也将写成有限多个不可约元的积. 这与 $a \in S$ 矛盾. 所以, b 或 c 属于 S, 从而 b 或 c 属于 $S(a)$. 所以 $S(a)$ 不是空集. 然后应用选择函数 f 构造出一个唯一的因子降链

$$a_0, a_1, a_2, \cdots \qquad a_{n+1}|a_n \tag{1}$$

而且

$$a_n \not\sim a_{n+1}, \quad n = 0, 1, 2, \cdots$$

令 $S_0 = S, a_0 = f(S_0)$. 由于 $S(a_0)$ 非空, 令 $a_1 = f(S(a_0))$. 由于 $a_1 \in S(a_0)$, $a_1|a_0$ 且 $a_1 \not\sim a_0$. 假设已构造出 S 的一个序列 $a_0, a_1, \cdots, a_n, a_{i+1}|a_i$ 且 $a_{i+1} \not\sim a_i$, $i = 0, 1, \cdots, n-1$. 由于 $S(a_n) \subset S$ 而且非空, 取 $a_{n+1} = f(S(a_n))$ 于是 $a_{n+1}|a_n$ 且 $a_{n+1} \not\sim a_n$. 根据归纳法构造, 于是构造出一个唯一的无限的因子降链 (1). 这与引理 1 的假设抵触. 因而 S 必须是空集. 所以 R 满足定义 2 中的条件 1). □

定理 2 设整环 R 满足条件

1) 因子链条件;

2) 每个不可约元都是素元;

则 R 是一个唯一因子分解整环.

证明 根据引理 1,R 的每个非零非单位的元素 a 都可分解成有限多个不可约元的乘积:

$$a = p_1 p_2 \cdots p_r,$$

因而 R 满足定义 2 中的条件 1). 至于 R 满足定义 2 中的条件 2), 即分解唯一性, 其证明几乎是完全重复整数环 $\mathbf{Z}$ 的算术基本定理中的唯一性的证明. 在这里就不重复了. 所以 R 是一个唯一因子分解整环. □

推论 主理想整环是唯一因子分解整环.

证明 根据 §1、引理 2 和引理 4 即得. □

我们知道, 在整数环和域上一元多项式环中从最大公因子的存在可以推出不可约元为素元这一事实. 这对于任一个最大公因子存在的整环也是成立的. 为此需要

引理 2 假设整环 R 的任一对元素都有最大公因子. 用 (a,b) 表示元素 a,b 的一个最大公因子, 则有 $c(a,b) \sim (ca,cb)$.

证明 当 $c=0$ 或 $(a,b)=0$ 时结论显然成立. 因此不妨设 $c \neq 0, (a,b) \neq 0$. 将 (a,b) 和 (ca,cb) 分别简记作 d 和 e. 一方面 $cd|ca, cd|cb$, 所以 $cd|e$. 于是 e 可表成 $e = cdu$. 我们证明 u 为单位. 事实上, $e|ca$, 设 $ca = ev$, 于是 $ca = cduv$, 因 $c \neq 0$, 可以消去 c, 得 $a = duv$. 同理 $b = duv'$, 因而 $du|(a,b)$, 于是 $du|d$, 设 $d = duu'$, 因 $d \neq 0$, 消去 d, 得 $1 = uu'$. 故 u 为单位. 所以 $e \sim cd$. □

引理 3 设整环 R 的每一对元素都有最大公因子, 则 R 的每个不可约元为素元.

证明 设 p 为任一不可约元, 假设 $p|ab$. 令 d 为 p, a 的一个最大公因子. 若 $d \sim p$, 则 $p|a$. 否则可设 $d=1$, 于是 $b = bd$ 为 bp 和 ba 的一个最大公因子 (引理 2). 由假设 p 为 bp 和 ab 的一个公因子. 从而 $p|b$. 总之, $p|a$ 或 $p|b$, 所以 p 为一个素元. □

定理 3 若整环 R 满足下列两条件

1) R 中因子链条件;

2) R 中每一对元素都有最大公因子;

则 R 是一个唯一因子分解整环.

证明 由定理 2 和引理 3 即得. □

设 R 为一个唯一因子分解整环. 于是 R 的每个非零非单位的元素 a 可以写成有限多个不可约元的积. 为了引进标准分解式, 在每个不可约元的相伴类

中取定一个代表，于是得到不可约元的相伴代表系，记作 S. 每个不可约元恰好与 S 中一个代表相伴，于是它可写成这个代表和一个单位的积. 这样 R 的每个非零元素 a 可以唯一地写成 S 中元素的方幂和一个单位的乘积

$$a = u\prod_{p_i\in S} p_i^{r_i},\ u\in U, \tag{2}$$

其中 $r_i \geq 0$ 而且除有限多个 r_i 外其余全为 0. (2) 叫做 a 的 **标准分解式**. 当然标准分解式依赖于相伴代表系的选取. 设 $b\in R, b\neq 0, b$ 的标准分解式为

$$b = u'\prod_{p_i\in S} p_i^{s_i},\ u'\in U.$$

不难证明下列事实:

1) $a|b \iff r_i\leq s_i$ 对所有 $p_i\in S$. 因而 $a\sim b \iff r_i = s_i$ 对所有 $p_i\in S$.

2) a 的因子分成相伴类，其类数有限. 实际上有 $\prod\limits_i (r_i+1)$ 类. 因此，因子降链条件在 R 中成立.

3) 令 $e_i = \min(r_i, s_i)$, 则 $d = u''\prod\limits_{p_i\in S} p_i^{e_i}$ 是 a,b 的最大公因子，其中 $u''\in U$.

4) 令 $m_i = \max(r_i, s_i)$, 则 $m = v\prod\limits_{p_i\in S} p_i^{m_i}$ 是 a,b 的最小公倍数，其中 $v\in U$.

由此可知，定理 2 和定理 3 的逆定理都成立.

在下一节将要看到，唯一因子分解整环比主理想整环要广泛得多. 后者作为前者的一个子类有如下的刻画.

定理 4 *一个唯一因子分解整环 R 是主理想整环的充要条件是 R 满足下列条件之一:*

1) 元素 $a,b\in R$ 的最大公因子恒可表成 a,b 的组合.

2) R 的每个不可约元生成的主理想为极大理想.

证明

1) 必要性由 §1 引理 3 导出. 下证充分性. 根据题设可知 R 中两个主理想的和仍为一个主理想 $(a)+(b)=(d)$, d 就是 a,b 的一个最大公因子. 设 N 为 R 的任一非零理想. 求证 N 为主理想. 首先在 N 内取定一个非零元素 a_1. 若差集 $N-(a_1)$ 非空，则在 $N-(a_1)$ 内取定一个元素 b_1, 令 $(a_1)+(b_1)=(a_2)$. 于是 $(a_1)\subset(a_2)$ 且 $(a_1)\neq(a_2)$. 若 $N-(a_2)$ 非空，则在 $N-(a_2)$ 内取定一个元素 b_2. 令 $(a_2)+(b_2)=(a_3)$, 于是 $(a_2)\subset(a_3)$ 且 $(a_2)\neq(a_3)$. 如此继续下去，最多 n 步后 $N-(a_n)$ 为空集，其中 n 不超过包含 (a_1) 的主理想的个数，这个数目等于 a_1 的相伴因子类的类数. 这就证明了 $N=(a_n)$.

2) 必要性由 §1 引理 2 导出. 下证充分性. 设 a,b 为 R 的不相伴的不可约元. 根据题设 (a) 和 (b) 是极大理想而且 $(a)\neq(b)$. 于是 $(a)+(b)=R$, 因而 $(a),(b)$ 互素. 其次设 a,b 为 R 的任意两个非零元, d 为 a,b 的一个最大公因子. 令 $a=da_1, b=db_1$. 则 a_1 的每个素因子和 b_1 的每个素因子不相伴, 因而它们分别生成的主理想互素. 重复地应用第三章 §2 的引理的 2), 理想 (a_1) 与 (b_1) 互素. 于是

$$(a)+(b)=(d)(a_1)+(d)(b_1)=(d)[(a_1)+(b_1)]=(d).$$

因此 a,b 的最大公因子可表成 a,b 的组合. 这就证明了 R 满足条件 1). 由 1) 的证明可知 R 为一个主理想整环. □

下面举一个唯一因子分解定理在其中不成立的整环.

例 设 $R=\mathbf{Z}[\sqrt{-5}]=\{a+b\sqrt{-5}\mid a,b\in\mathbf{Z}\}$. R 是 $\mathbf{Q}(\sqrt{-5})$ 的代数整数环. 我们指出 R 中存在不可约元, 但非素元. 首先决定 R 的单位. 设 $\alpha=a+b\sqrt{-5}$ 是一个单位, 则存在一个 $\beta=c+d\sqrt{-5}$ 使得 $\alpha\beta=1$. 取范数得 $1=N(\alpha\beta)=N(\alpha)\cdot N(\beta)$. 由于 $N(\alpha),N(\beta)$ 为正整数, 推出 $N(\alpha)=1$, 即 $a^2+5b^2=1$. 从而 $b=0, a=\pm1$. 所以 R 仅有单位 ±1. 因此, R 的元素 α,β 相伴的充要条件是 $\alpha=\pm\beta$. 6 在 R 中有两种分解

$$6=2\cdot3=(1+\sqrt{-5})(1-\sqrt{-5}).$$

我们证明 2,3 和 $1\pm\sqrt{-5}$ 都是 R 的不可约元. 设 $1+\sqrt{-5}$ 有分解 $1+\sqrt{-5}=(a+b\sqrt{-5})(c+d\sqrt{-5})$. 取范数得 $6=(a^2+5b^2)(c^2+5d^2)$. 从而推出 $a^2+5b^2=2, c^2+5d^2=3$ 或 $a^2+5b^2=1, c^2+5d^2=6$(还有两种情况与此对称). 前者不可能, 只能是 $a^2+5b^2=1$ 或 $c^2+5d^2=1$. 从而推出 $a+b\sqrt{-5}=\pm1$ 或 $c+d\sqrt{-5}=\pm1$. 所以 $1+\sqrt{-5}$ 是不可约元. 同理可证 $1-\sqrt{-5}$, 2 和 3 都是不可约元. 而且它们彼此不相伴. 同时也说明 6 和 $2(1+\sqrt{-5})$ 的公因子只有 ±2 和 $\pm(1+\sqrt{-5})$, 但它们都不是最大公因子.

说明 上面例子告诉我们, 整数环 $\mathbf{Z}$ 的算术基本定理不能推广到二次数域的代数整数环上去. 但是将关于元素的算术基本定理换写成关于理想的定理 "整数环 $\mathbf{Z}$ 的任一非零非单位理想 (n) 恒可唯一地写成一些素理想 (p_i) 的方幂的乘积 $(n)=(p_1)^{e_1}\cdots(p_r)^{e_r}$". 那么它就可以推广到 R_m 上去. 戴德金 (Dedekind) 根据库默尔 (Kummer) 的理想数朴素思想提出了现代形式的理想概念; 并且成功地证明了关于代数整数环的算术基本定理: "在数域的代数整数环中任一非零非单位理想 A 恒可唯一地写成一些素理想 p_i 的方幂的乘积 $A=p_1^{e_1}\cdots p_r^{e_r}$". 就上面的例子来说, 在 R_{-5} 中 6 有两种分解 $6=2\cdot3=(1+\sqrt{-5})(1-\sqrt{-5})$.

把它写成理想的形式有

$$(6) = (2)\cdot(3) = (1+\sqrt{-5})\cdot(1-\sqrt{-5}),$$

就会发现理想 $(2),(3),(1+\sqrt{-5})$ 和 $(1-\sqrt{-5})$ 并非极大理想，而是可以进一步分解的．实际上，令

$$P_1 = (2, 1+\sqrt{-5}),\quad P_2 = (3, 1+\sqrt{-5}),$$
$$P_3 = (2, 1-\sqrt{-5}),\quad P_4 = (3, 1-\sqrt{-5}).$$

不难证明 $P_1,\cdots,P_4$ 都是 R_{-5} 的极大理想，而且有下列分解：

$$(2) = P_1\cdot P_3,\ (3) = P_2\cdot P_4,\ (1+\sqrt{-5}) = P_1\cdot P_2,\ (1-\sqrt{-5}) = P_3\cdot P_4,$$

于是 (6) 就得到最后的分解

$$(6) = P_1P_2P_3P_4.$$

§4 高斯整环的多项式扩张

在高等代数里已经知道，唯一因子分解定理可以从整数环 **Z** 推广到它上面的一元多项式环．这种推广带有普遍性，就是说，高斯整环上一元多项式环仍然是高斯整环．

设 R 为一高斯整环，$R[x]$ 为 R 上一元多项式环，$f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$，用 $(a_0, a_1, \cdots, a_n)$ 表示 $a_0, a_1, \cdots, a_n$ 的一个最大公因子．$(a_0, a_1, \cdots, a_n)$ 叫做 $f(x)$ 的 **容度**，记做 $c(f) = (a_0, a_1, \cdots, a_n)$，$c(f)$ 在相伴意义下由 $f(x)$ 唯一决定．

如果 $c(f) \sim 1$，则 $f(x)$ 叫做一个 **本原多项式**，$R[x]$ 中的单位是零次本原多项式，$R[x]$ 中的一个不可约元或者是 R 中一个不可约元或者是一个正次数多项式，如为后者，则它是一个容度为 1 的不可约多项式，也就是一个不可约的本原多项式．反之，一个不可约的本原多项式是 $R[x]$ 的一个不可约元．

引理 1 *$R[x]$ 中任一个非零多项式 $f(x)$ 恒可写成一个常数 d 和一个本原多项式 $f_1(x)$ 的积，而且 d 和 $f_1(x)$ 在相伴意义下由 $f(x)$ 唯一决定．*

证明 设 $f(x) = a_0 + a_1x + \cdots + a_nx^n$，令 $d = c(f) = (a_0, a_1, \cdots, a_n), a_i = a_i'd$. $f_1(x) = a_0' + a_1'x + \cdots + a_n'x^n$．于是 $f(x) = d\cdot f_1(x)$，$f_1(x)$ 为本原多项式．设 $f(x) = e\cdot f_2(x)$ 为任一分解，$e \in R$，$f_2(x)$ 为本原，令 $f_2(x) = b_0 + b_1x + \cdots + b_nx^n$．由于

$$c(f) \sim (da_0', da_1', \cdots, da_n') \sim d(a_0', a_1', \cdots, a_n') \sim d.$$

同样 $c(f)\sim(eb_0,eb_1,\cdots,eb_n)\sim e(b_0,b_1,\cdots,b_n)\sim e$. 所以 $d\sim e$. 令 $e=ud$, u 为单位. 于是 $f_1(x)=uf_2(x)$, $f_1(x)\sim f_2(x)$. □

根据引理 1, 分解 $f(x)$ 可以分别对常数 d 和本原多项式进行分解. d 在 R 中的分解, 存在性和唯一性已不成问题, 一个正次数本原多项式在 $R[x]$ 中分解成有限多个不可约元的积, 这种存在性也没有问题, 问题在于分解的唯一性. 为了证明唯一性, 需要解决两个问题:

1) $R[x]$ 的本原多项式集合对乘法封闭;

2) 设 F 为 R 的商域, $R[x]$ 中一个正次数不可约多项式是否在 $F[x]$ 中也不可约? (根据第三章 §6 定理 14 的推论可知 $R[x]$ 可以嵌入 $F[x]$ 中, 作为 $F[x]$ 的一个子环.)

引理 2 (高斯引理) *本原多项式的积仍为本原多项式.*

证明 设 $f(x)=a_0+a_1x+\cdots+a_mx^m$ 和 $g(x)=b_0+b_1x+\cdots+b_nx^n$ 为两个本原多项式, 令 $f(x)\cdot g(x)=h(x)$. 反证法. 假若 $h(x)$ 非本原, 则将存在 R 的一个不可约元 p 整除 $c(h)$. 由于 $f(x)$ 为本原, 可设 a_r 是 $a_0,a_1,\cdots$ 中最前一个不被 p 整除的. 同样, 设 b_s 是 $b_0,b_1,\cdots$ 中最前一个不被 p 整除的. 考虑 $h(x)$ 的 x^{r+s} 项的系数 c_{r+s}

$$c_{r+s}=a_0b_{r+s}+\cdots+a_{r-1}b_{s+1}+a_rb_s+a_{r+1}b_{s-1}+\cdots+a_{r+s}b_0,$$

在上式中 a_rb_s 一项不被 p 整除外, 其余各项都被 p 整除, 因而 p 不能整除 c_{r+s}, 这与 $p|c(h)$ 矛盾. 所以 $h(x)$ 为本原. □

引理 3 *设 F 为高斯整环 R 的商域, $R[x]$ 根据第三章定理 14 的推论看作 $F[x]$ 的一个子环. 于是*

1) 设 $f(x)$ 和 $g(x)$ 为 $R[x]$ 的任两个本原多项式. 则 $f(x)$ 和 $g(x)$ 在 $R[x]$ 中相伴当且仅当 $f(x),g(x)$ 在 $F[x]$ 中相伴.

2) $F[x]$ 中任一非零多项式 $f(x)$ 恒可表成 $f(x)=\dfrac{d}{e}\cdot g(x)$, $d,e\in R$, $g(x)$ 为 $R[x]$ 本原多项式, 而且在 $R[x]$ 中相伴意义下 $g(x)$ 由 $f(x)$ 唯一决定.

证明 1) 若 $f(x)$ 和 $g(x)$ 在 $R[x]$ 中相伴, 则它们自然在 $F[x]$ 中相伴. 反之, 设 $f(x),g(x)$ 在 $F[x]$ 中相伴, 即 $f(x)$ 可写成 $f(x)=\dfrac{a}{b}g(x)$, $a,b\in R$, $a\neq0$, $b\neq0$, 于是 $bf(x)=ag(x)$, 根据引理 1, 在 $R[x]$ 中有 $a\sim b$. 于是 $a=u\cdot b$, u 为 R 的一个单位. 因而 $f(x)=ug(x)$. 即 $f(x),g(x)$ 在 $R[x]$ 中相伴.

2) 设 $f(x)=\dfrac{a_0}{b_0}+\dfrac{a_1}{b_1}x+\cdots+\dfrac{a_n}{b_n}x^n\in F[x]$, $a_i,b_i\in R$, $f(x)\neq0$, 令 e 表示 $b_0,\cdots,b_n$ 的一个最小公倍, 于是 $f(x)=\dfrac{1}{e}\cdot f_1(x)$, $f_1(x)\in R[x]$. 根据引理 1, $f_1(x)$ 可写成 $f_1(x)=dg(x)$, $d\in R$, $g(x)$ 为本原多项式, 于是 $f(x)=\dfrac{d}{e}g(x)$.

设 $f(x)$ 还可写成 $f(x)=\frac{a}{b}h(x), a,b\in R$, $h(x)$ 为 $R[x]$ 的一个本原多项式. 则 $g(x),h(x)$ 在 $F[x]$ 中相伴. 根据 1) 它们在 $R[x]$ 中也相伴. □

推论 若一个正次数本原多项式 $g(x)$ 在 $R[x]$ 中不可约, 即不能写成两个正次数多项式的积, 则 $g(x)$ 在 $F[x]$ 中也不可约.

证明 反证法. 假设 $g(x)$ 在 $F[x]$ 中可约. 设 $g(x)=f_1(x)\cdot f_2(x), f_i(x)\in F[x], \deg f_i(x)>0$. 根据引理 3,2), $f_i(x)$ 可表成

$$f_i(x)=\alpha_i g_i(x),\quad i=1,2,$$

其中 $\alpha_i\in F, g_i(x)\in R[x]$ 为本原, 于是

$$g(x)=\alpha_1\alpha_2 g_1(x)g_2(x).$$

根据引理 2, $g_1(x)g_2(x)$ 为本原. 根据引理 3,1), $g(x)$ 和 $g_1(x)\cdot g_2(x)$ 在 $R[x]$ 中相伴, 即 $\alpha_1\alpha_2\in R$, 而且 $\deg g_i(x)>0$, 这与 $g(x)$ 在 $R[x]$ 中不可约矛盾. □

设 R 的任一非零元素 a 分解成 $a=f(x)\cdot g(x), f(x),g(x)\in R[x]$. 由于 R 为整环, 根据次数性质有 $0=\deg f(x)+\deg g(x)$, 从而 $\deg f(x)=\deg g(x)=0$, 即 $f(x),g(x)\in R$. 由此可知 a 在 $R[x]$ 中进行分解实际上是在 R 中进行分解, 而且 R 的不可约元也是 $R[x]$ 的不可约元. 另外, $R[x]$ 的任一本原多项式 $f(x)$ 的任一因式显然还是本原多项式. 因此, 任一本原多项式在 $R[x]$ 内进行分解实际上是在本原多项式集合中进行分解.

定理 5 高斯整环 R 上的一元多项式环仍为一高斯整环.

证明 设 $f(x)$ 为 $R[x]$ 的任一多项式, $f(x)\neq 0$ 而且非单位. 根据引理 1, $f(x)=dg(x), d\in R, g(x)$ 为一本原多项式. 根据上面的说明, 若 d 非单位, 则 d 在 $R[x]$ 中分解成不可约元 $p_1,\cdots,p_t$ 之积, 且 $p_i\in R$. 若 $g(x)$ 为一正次数多项式而且分解成 $g(x)=g_1(x)\cdot g_2(x), \deg g_i(x)>0$. 由于 R 为整环, $\deg g(x)=\deg g_1(x)+\deg g_2(x), \deg g_i(x)<\deg g(x)$. 因此对 $g(x)$ 的次数作归纳法可证 $g(x)$ 可分解成本原的不可约多项式 $q_1(x),\cdots q_r(x)$ 之积而且 $\deg q_i(x)>0$, 于是 $f(x)$ 最后分解成 $R[x]$ 的不可约元的乘积

$$f(x)=p_1\cdots p_t q_1(x)\cdot q_r(x).$$

其次, 证明分解的唯一性. 设

$$f(x)=p_1'p_2'\cdots p_m'q_1'(x)q_2'(x)\cdots q_s'(x)$$

为任一分解, 其中 p_i' 为 R 的不可约元, $q_j'(x)$ 为 $R[x]$ 的正次数不可约本原多项式. 根据引理 2, $\prod\limits_i q_i(x)$ 和 $\prod\limits_i q_i'(x)$ 都是本原多项式. 根据引理 1, 得

$$\prod p_i\sim\prod p_i',\quad \prod q_i(x)\sim\prod q_i'(x),$$

即

$$p_1'p_2'\cdots p_m' = up_1p_2\cdots p_t$$

和

$$q_1'(x)q_2'(x)\cdots q_s'(x) = vq_1(x)q_2(x)\cdots q_r(x),$$

其中 u, v 为单位. 由于 R 为高斯整环, 从前一式得 $m = t$, p_i' 的脚标作适当改写可使 $p_i' \sim p_i$, $i = 1, 2, \cdots, t$. 将后一式放到 $F[x]$ 内去考虑, F 为 R 的商域. 根据引理 3 的推论, 这些 $q_i(x), q_i'(x)$ 在 $F[x]$ 内仍不可约. 于是 $r = s$, 适当改换 $q_i'(x)$ 的脚标可使 $q_i'(x)$ 和 $q_i(x)$ 在 $F[x]$ 内相伴. 根据引理 3,1),$q_i'(x)$ 和 $q_i(x)$ 在 $R[x]$ 内也相伴. 这就证明了分解的唯一性. 所以 $R[x]$ 为一高斯整环. □

推论 *设 R 为一个高斯整环, 则 R 上 (n 个未定元的) 多元多项式环 $R[x_1, \cdots, x_n]$ 也是高斯整环.*

一个域 F 上的一元多项式环 $F[x]$ 有无限多个互不相伴的不可约多项式. 但是一般不易判断一个给定的多项式是否是不可约的. 如果 F 是一个高斯整环 R 的商域, 那么我们根据本原多项式的理论, 利用 R 的不可约元可以明确地作出 $F[x]$ 的一类重要的不可约多项式.

定理 6 (艾森斯坦判别法) *设 F 为一高斯整环 R 的商域, $F[x]$ 为 F 上一元多项式环. 设 $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$, $a_n \neq 0, n > 1$. 若 R 有一个不可约元 p 满足:*

1) $p|a_i$, $i = 0, 1, \cdots, n-1$;

2) $p^2 \nmid a_0, p \nmid a_n$;

则 $f(x)$ 在 $F[x]$ 内不可约, 换句话说 $f(x)$ 在 $R[x]$ 内不能写成两个正次数多项式的积.

证明 反证法. 假设 $f(x) = g(x)h(x)$,

$$g(x) = b_0 + b_1x + \cdots + b_rx^r,\quad b_i \in R, b_r \neq 0, r > 0,$$
$$h(x) = c_0 + c_1x + \cdots + c_sx^s,\quad c_i \in R, c_s \neq 0, s > 0.$$

由于 R 为整环, $r < n, s < n$. 由于 $p|a_0$ 但 $p^2 \nmid a_0$, b_0 和 c_0 恰有一个被 p 整除. 不妨设 $p \nmid b_0, p|c_0$. 又因 $p \nmid a_n$, 所以 $p \nmid b_r, p \nmid c_s$. 设 c_j 是 $c_0, \cdots, c_s$ 中第一个不能被 p 整除的, 则 $0 < j \leq s$. 考虑 a_j,

$$a_j = b_0c_j + b_1c_{j-1} + \cdots + b_jc_0$$

在上式右端 b_0c_j 不被 p 整除, 但其余各项都被 p 整除, 因而 $p \nmid a_j$. 可是 $j \leq s < n$, 这与题设矛盾. □

满足定理 6 中条件的多项式叫做 **艾森斯坦** (Eisenstein) **多项式**.

例 1 对于任一素数 p 和正整数 $n, x^n - p$ 是 $\mathbf{Z}[x]$ 中的艾森斯坦多项式. 因而在 $\mathbf{Q}[x]$ 中不可约.

例 2 在高斯整数环 $R_{-1} = \mathbf{Z}[\sqrt{-1}]$ 中令 $\pi = 1 - \sqrt{-1}$. 范数 $N(\pi) = 2$, 由此可以证明 π 是 R_{-1} 的一个不可约元. 令 $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + \pi$. 让 $a_1, \cdots, a_{n-1}$ 取在主理想 (π) 内, 则 $f(x)$ 就是 $\mathbf{Q}(\sqrt{-1})$ 上的不可约多项式.

§5 希尔伯特基定理

在这一节简单介绍诺特 (E.Noether) 环. 它是一类相当广泛的环. 而且把很多重要类型的环都包括在内.

定义 3 如果一个交换环 R 的每个理想升链

$$N_1 \subset N_2 \subset \cdots$$

都有限, 即存在一个正整数 m 使得

$$N_m = N_{m+1} = N_{m+2} = \cdots$$

则称 R 满足理想升链条件. 如果一个交换环 R 满足理想升链条件, 则 R 叫做**诺特环**.

主理想环, 特别是整数环和域上一元多项式环都是诺特环. 二次数域 $\mathbf{Q}(\sqrt{m})$ 的代数整数环 R_m 也是诺特环.

如果一个交换环 R 的由理想组成的任一个非空集合 (按包含关系是一个偏序集) 都有极大元, 则称 R 满足关于理想的极大条件或简称 R 满足**极大条件**.

定理 7 *对于任一交换环 R 来说, 下列叙述等价:*

1) R 是一个诺特环;

2) R 满足理想的极大条件;

3) R 的每个理想都是有限生成的.

证明 1) $\Rightarrow$ 2). 反证法. 假设存在 R 的理想构成的一个非空的集合 S, 使得 S 按包含关系没有极大元. 令 P 表示 S 的一切非空子集构成的集, f 表示 P 上的一个选择函数. 根据 f 可构造出 R 的一个无限的严格递升的理想链

$$N_1 \subset N_2 \subset \cdots, \quad N_i \neq N_{i+1},\ i = 1, 2, \cdots \tag{1}$$

首先取 $N_1 = f(S)$. 令 S_1 表示 S 中真包含 N_1 的一切理想构成的子集. 由于 S 没有极大元, S_1 不是空集; 而且 S_1 也没有极大元. 因为, 若 S_1 是空集, 则 N_1 将是 S 的一个极大元, 这与关于 S 的假设抵触; 若 S_1 有一个极大元 A, 则

A 将也是 S 的一个极大元. (因为若 $A \subset B$ 对某一个 $B \in S$, 将有 $N_1 \subset B$, 从而 $B \in S_1$. 根据 A 为 S_1 的极大元, 推出 $B = A$, A 将是 S 的一个极大元.) 这又与 S 的假设抵触. 然后取 $N_2 = f(S_1)$. 于是 $N_1 \subset N_2$ 但 $N_1 \neq N_2$. 重复上面的方法. 从 N_2 构造出 N_3. 于是递归地可以构造出一个无限的严格递升的理想链 (1). 这与 1) 抵触. 所以 2) 成立.

2) $\Rightarrow$ 3). 设 N 为 R 的任一个理想, 求证 N 有限生成. 设 S 是由 N 的一切有限子集生成的理想所构成的集合. 根据题设, S 有一个极大元. 设 A 是它的一个极大元. 于是 $A \subset N$ 而且 A 有限生成. 求证 $A = N$. 假若 $A \neq N$, 则将存在一个元素 $a \in N$ 但 $a \notin A$. 作 $B = A + (a)$. $A \subset B$, $A \neq B$. 这与 A 为 S 的极大元抵触. 所以 $N = A$ 是有限生成的. 因而 3) 成立.

3) $\Rightarrow$ 1). 设

$$N_1 \subset N_2 \subset \cdots, \quad N_i \subset N_{i+1}, \; i = 1, 2, \cdots \tag{2}$$

为 R 的任一个理想升链, 求证它有限. 令 $N = \bigcup_i N_i$. 由于 (2) 是一个升链, 易知 N 是一个理想. 根据 3)N 是有限生成的. 设 $N = (a_1, \cdots, a_r)$. 根据 N 的作法, 每个 a_i 属于某一个 N_{n_i} $(i = 1, \cdots, r)$. 设 n 为 $n_1, \cdots, n_r$ 的最大者. 于是 $a_i \in N_n, i = 1, \cdots, r$. 从而 $N \subset N_n$. 由于 $N \subset N_n \subset N_{i+n} \subset N$ 对所有 $i \geq 0$, 最后得 $N = N_n = N_{n+1} = \cdots$. 所以 1) 成立. □

根据第三章 §§1,2,5 的结果, 可以证明 (留作习题):

1) 诺特环的商环为诺特环;

2) 若交换环 R 有一个理想 N 使得商环 R/N 和 N 都是诺特环, 则 R 本身也是诺特环;

3) 有限多个诺特环的直和为诺特环;

4) 诺特环 (有单位元素) 的分式环为诺特环.

但是诺特环的子环不必是诺特环.

定理 8 (希尔伯特 (Hilbert) 基定理) *如果 R 是一个诺特环而且有单位元素, 则 R 上的一元多项式环 $R[x]$ 也是诺特环.*

证明 设 H 为 $R[x]$ 的任一理想, 求证 H 有限生成. 先作 R 的一串理想. H 中所有 r 次多项式的首项系数加上零组成的集合记作 I_r, $r = 0, 1, \cdots$. I_r 是一个理想, 因为, 对于 $a, b \in I_r, a \neq 0, b \neq 0$, 存在 r 次多项式 $f(x) = ax^r + \cdots$ 和 $g(x) = bx^r + \cdots$ 属于 H. 于是 $f(x) - g(x) = (a - b)x^r + \cdots$ 也属于 H. $a - b \neq 0$ 或 $a - b = 0$, 总之, $a - b \in I_r$. 对于任一 $c \in R$, $cf(x) = cax^r + \cdots \in H$, $ca \neq 0$ 或 $ca = 0$, 总之 $ca \in I_r$. 其次, 若 $f(x) = ax^r + \cdots \in H$, 则 $xf(x) = ax^{r+1} + \cdots \in H$. 因此, 若 $a \in I_r$, 则 $a \in I_{r+1}$. 于是 $\{I_r\}$ 构成一个理想升链. 因为 R 是诺特环,

存在一个非负整数 m 使得

$$I_m = I_{m+1} = I_{m+2} = \cdots$$

而且 $I_0, I_1, \cdots, I_m$ 都是有限生成的．设

$$I_r = (a_{r1}, \cdots, a_{rn_r}), \quad r = 0, 1, \cdots, m.$$

于是在 H 中存在 r 次多项式 $f_{ri}(x)$, 其首项系数为 a_{ri}, $i = 1, \cdots, n_r$, $r = 0, 1, \cdots, m$. 求证 $\{f_{ri}(x)\}$ 是 H 的一组生成元.

我们来证明 H 中任一多项式 $f(x)$ 可表成 $f_{ri}(x)$ 的组合．若 $f(x) = 0$, 显然．设 $f(x) \neq 0$. 对 $f(x)$ 的次数作归纳法．假设若 $\deg f(x) < r$, 则 $f(x)$ 可表成 $f_{ri}(x)$ 的组合．设 $f(x) = ax^r + \cdots, a \neq 0$. 若 $r \geq m$, 则 $a \in I_r = I_m$, a 可表成 $a_{m1}, \cdots, a_{mn_m}$ 的组合. 设 $a = \sum_{i=1}^{r_m} b_i a_{mi}$. 令 $g(x) = \sum_{i=1}^{r_m} b_i x^{r-m} f_{mi}$. 于是 $g(x) \in H$ 且与 $f(x)$ 有相同的首项．令 $f_1(x) = f(x) - g(x)$. 则 $\deg f_1(x) < r$. 若 $r < m$, 则 $a \in I_r, 0 \leq r < m$. 于是 a 可表成 $a = \sum_{i=1}^{r_n} c_i a_{ri}$. 同样令 $g(x) = \sum_{i=1}^{r_n} c_i f_{ri}(x)$, 则 $g(x) \in H$ 且与 $f(x)$ 有相同的首项．令 $f_1(x) = f(x) - g(x)$. 则 $\deg f_1(x) < r$. 总之， $f(x) = g(x) + f_1(x)$, $f_1(x) \in H$ 且 $\deg f_1(x) < r$. 根据归纳法假设， $f_1(x)$ 可以表成 $f_{ri}(x)$ 的组合．因而 $f(x)$ 也可表成 $f_{ri}(x)$ 的组合．所以 $f_{ri}(x)$ 是 H 的一组生成元，即 H 是有限生成的． □

推论 1 *设 R 是一个有单位元素的诺特环，则 R 上有限多个未定元的多项式环也是诺特环.*

证明 对未定元的个数作归纳法即得． □

推论 2 *设 R 为一个有单位元素的诺特环， $R[u_1, \cdots, u_r]$ 为 R 上有限生成的交换环且与 R 有相同的单位元素．于是 $R[u_1, \cdots, u_r]$ 是一个诺特环，而且 $u_1, \cdots, u_r$ 在 R 上的全部代数关系在多项式环 $R[x_1, \cdots, x_r]$ 中是有限生成的.*

证明 设 $R[x_1, \cdots, x_r]$ 为 R 上 r 个未定元的多项式环．根据第三章 §6 定理 15 的推论 1, 存在 $R[x_1, \cdots, x_r]$ 到 $R[u_1, \cdots, u_r]$ 的同态 σ 使得 σ 限制在 R 上为恒等映射且 $\sigma(x_i) = u_i$, $i = 1, \cdots, r$. 设 $I = \ker(\sigma)$. 根据第三章 §1 定理 1,$R[x_1, \cdots, x_r]$ 中包含 I 的理想与 $R[u_1, \cdots, u_r]$ 的理想在 σ 下成一一对应: $H \to \sigma(H)$. 因为 $R[x_1, \cdots, x_r]$ 为诺特环, H 是有限生成的, 设 $H = (f_1, \cdots, f_s)$. 则 $\sigma(H) = (\sigma(f_1), \cdots, \sigma(f_s))$ 也是有限生成的．所以 $R[u_1, \cdots, u_r]$ 为诺特环．其次， σ 的核 I 是元素 $u_1, \cdots, u_r$ 在 R 上的代数关系的总和． I 是 $R[x_1, \cdots, x_r]$ 的一个理想，当然是有限生成的． □

整数环上有限多个未定元的多项式环 $\mathbf{Z}[x_1,\cdots,x_r]$ 和域 F 上有限多个未定元的多项式环 $F[x_1,\cdots,x_r]$ 是两类重要的诺特环. 上述基定理, 首先是由希尔伯特就这两种情况证明的.

说明 在 §3 末只是简单地介绍了如何将整数环的算术基本定理推广到代数整数环 (读者记住二次数域的代数整数环就够了), 其中代数整数环保留了整数环关于理想的几乎一切性质. (每个理想为主理想这一条除外) 本节所作的从整数环和域上一元多项式环到诺特环的推广, 则是最为广泛的一次推广. 诺特环只保留整数环的一条性质即理想升链条件. 那么我们进一步要问, 整数环的算术基本定理如何推广到诺特环上? 由于整数环中非零素理想都是极大理想, 不同非零素理想的方幂彼此互素, 因而不同素理想方幂的乘积可以写成它们的交的形式. 因此整数环的算术基本定理又可表成: "整数环 $\mathbf{Z}$ 的每个非零非单位理想 A 可以唯一地写成有限多个素理想方幂的交 $A=P_1^{e_1}\cap P_2^{e_2}\cap\cdots\cap P_r^{e_r}$, 而每个 $P_i^{e_i}$ 则不能写成两个真包含 $P_i^{e_i}$ 的理想的交." 保留素理想方幂的后一个性质, 在诺特环中引进不可约理想的概念, 则上述定理就可以推广到诺特环.

设 R 为一个诺特环. A,B 为 R 的理想. 如果 $A\subset B$, 则 B 叫做 A 的因子. 若 $A\subset B$ 且 $A\neq B$, 则 B 叫做 A 的一个真因子. 如果理想 A 不能写成两个真因子的交, 则 A 叫做**不可约的**. 否则叫做**可约的**.

例 1 整数环 $\mathbf{Z}$ 中 (0) 和非零素理想方幂 $(p)^e$ 都是不可约的.

例 2 在一元多项式环 $R=\mathbf{Z}[x]$ 中 $P=(2,x^2+x+1)$ 是 R 的一个极大理想. 因而 P 是不可约的. 但是 $P^2=(2^2,2(x^2+x+1),(x^2+x+1)^2)$ 则是可约的. 因为

$$P^2=(2,(x^2+x+1)^2)\cap(2^2,(x^2+x+1)).$$

定理 9 *诺特环 R 的每个理想都是有限多个不可约理想的交.*

证明 反证法. 假设存在一个理想, 它不能写成有限多个不可约理想的交. 则所有这样的理想构成的集合 S 不是空集. 根据极大条件, S 有一个极大元, 设 A 是 S 的一个极大元. 因为 A 可约, A 可写成两个真因子 B,C 的交 $A=B\cap C$. 由于 B,C 是 A 的真因子, B,C 不属于 S. 因而它们都可写成有限多个不可约理想的交. 设 $B=B_1\cap\cdots\cap B_r, C=C_1\cap\cdots\cap C_s$, B_i,C_j 为不可约理想. 于是 $A=B\cap C=B_1\cap\cdots\cap B_r\cap C_1\cap\cdots\cap C_s$. 这与 $A\in S$ 抵触. 所以 S 为空集. 就是说, R 的每个理想都是有限多个不可约理想的交. □

定理 9 以后给我们留下的问题都不能在这里讨论了.

上面已经提到, 整数环上和域上有限多个未定元的多项式环是诺特环的两种重要类型. 作为一个例子, 我们来决定 $\mathbf{Z}[x]$ 的素理想和极大理想. $\mathbf{Z}[x]$ 简记作 R.

我们已经知道，R 的一个非零主理想 $(f(x))$ 是素理想当而且仅当 $f(x)$ 是一个不可约元. 可以证明，R 的任一个主理想都不是极大理想，它作为习题 (本章习题 9) 请读者自己证明之.

其次，设 I 为 R 的一个素理想但非主理想. 则 $I \neq (0)$. 在 $I^* = I - \{0\}$ 中所有次数最低的多项式中取一个首项系数 > 0 且为最小的多项式 $p_0(x)$. 作差集 $S = I - (p_0(x))$. 根据假设，S 非空. 于是在 S 中取一个次数最低的多项式 $p_1(x)$. 显然 $\deg p_1(x) \geq \deg p_0(x)$. 由于 I 为素理想，$p_0(x)$ 是一个不可约元. 因为，设 $p_0(x) = f(x) \cdot g(x)$, $f(x)$ 和 $g(x)$ 的首项系数 > 0, 则 $f(x)$ 或 $g(x)$ 属于 I. 不妨设 $f(x) \in I$. 由 $p_0(x)$ 的选取，$\deg f(x)$ 不小于 $\deg p_0(x)$, 它们只能相等. 从而 $f(x)$ 的首项系数不小于 $p_0(x)$ 的首项系数，它们也只能相等，由此推出 $g(x) = 1$. 其次证明 $\deg p_0(x) = 0$. 假若 $\deg p_0(x) > 0$, 则任何非零整数不属于 $(p_0(x)), p_1(x)$ 也不属于 $(p_0(x))$. 于是 $p_0(x) \nmid kp_1(x)$ 对所有非零整数 k. 设 $p_0(x)$ 的首项系数为 a, 取一个整数 $u > \deg p_1(x) - \deg p_0(x)$. 让 $p_0(x)$ 对 $a^u p_1(x)$ 作除法算式，可以一直除到余数 $r(x)$ 的次数小于 $p_0(x)$ 的次数为止. 于是

$$a^u p_1(x) = q(x)p_0(x) + r(x).$$

我们有 $q(x), r(x) \in R$ 而且 $r(x) \neq 0, \deg r(x) < \deg p_0(x)$. 另一方面，$r(x) = a^u p_1(x) - q(x)p_0(x) \in I$. 这与 $p_0(x)$ 的选取矛盾. 所以 $\deg p_0(x) = 0$, 即 $p_0(x)$ 为一个素数. $p_0(x)$ 简记作 p. 由于 $\mathbf{Z}p \subset I \cap \mathbf{Z}$ 且 $I \cap \mathbf{Z} \neq \mathbf{Z}$, 有 $I \cap \mathbf{Z} = \mathbf{Z}p$. 又由于 $p_1(x) \notin (p)$, 从而 $p_1(x) \notin \mathbf{Z}, \deg p_1(x) > 0$. 我们进一步证明 $p_1(x)$ 还是 mod (p) 不可约的. 假若 $p_1(x) \equiv f(x) \cdot g(x) \pmod{(p)}$, $f(x)$ 和 $g(x)$ 次数都低于 $p_1(x)$ 的次数. 于是由 $p_1(x) \in I$ 导出 $f(x) \cdot g(x) \in I$, 从而 $f(x)$ 或 $g(x)$ 属于 I, 另一方面 $p_1(x) \notin (p)$, 从而 $f(x)g(x) \notin (p)$, $f(x)$ 和 $g(x)$ 都不属于 (p). 因而 $f(x)$ 或 $g(x)$ 属于 S. 这与 $p_1(x)$ 的取法矛盾. 由此同时证明了 $p_1(x)$ 的首项系数与 p 互素. 最后证明 $I = (p, p_1(x))$. 令 $N = (p, p_1(x))$. 求证 N 为极大理想即够. 根据第三章定理 2 有

$$R/N \cong R/(p)/N/(p).$$

根据第三章定理 15, 推论 2,$R/(p) \cong (\mathbf{Z}/\mathbf{Z}p)[\overline{x}], \overline{x} = x + (p)$. 设 $p_1(x) = a_0x^r - a_1x^{r-1} + \cdots + a_r$. 在同态 $R/(p) \to (\mathbf{Z}/\mathbf{Z}p)[\overline{x}]$ 下，$p_1(x) \mapsto \overline{p}_1(\overline{x}) = \overline{a}_0\overline{x}^r - \overline{a}_1\overline{x}^{r-1} + \cdots + \overline{a}_r$, $\overline{a}_i$ 是在自然同态 $\mathbf{Z} \to \mathbf{Z}/\mathbf{Z}p$ 下 a_i 的象. 于是最后得 $R/N \cong R/(p)/N/(p) \cong (\mathbf{Z}/\mathbf{Z}p)[\overline{x}]/(\overline{p}_1(\overline{x}))$, 其中 $N/(p) = (\overline{p}_1(\overline{x}))$. 根据第三章定理 21, 上式右端为一域. 因而 R/N 为一域. 根据第三章定理 7,N 为一个极大理想. 从 $N \subset I$ 且 $I \neq R$ 得 $N = I$.

反之，任给一个素数 p 和一个首项系数与 p 互素的正次数整系数多项式

$f(x)$, 若 $f(x) \pmod{(p)}$ 不可约, 则由 p 与 $f(x)$ 生成的理想是 $\mathbf{Z}[x]$ 的一个极大理想.

综上所述, $\mathbf{Z}[x]$ 的素理想可以分成三类:

1) 零理想;

2) 由不可约元生成的主理想. 但这一类素理想都不是极大理想;

3) 任给一个素数 p 和一个首项系数与 p 互素的正次数整系数多项式 $f(x)$ 而且模 (p) 是不可约的, 由 p 和 $f(x)$ 生成的理想 $(p, f(x))$, 这一类理想不仅是素理想而且是极大理想.

在第三类的素理想中, $(p, f(x)) = (q, g(x))$ 的充要条件是 $p = q$ 而且 $f(x) \equiv cg(x) \pmod{(p)}$, $c \in \mathbf{Z}$.

习　题

1. 设 D 为一个主理想整环而且包含在一个整环 R 内. 设 $a, b \in D$. 证明, 若 d 是 a, b 在 D 中的最大公因子, 则 d 也是 a, b 在 R 内的最大公因子.

2. 设 D 为一主理想整环, $a \in D$, $a \neq 0$. 若 a 为素元, 则 $D/(a)$ 为一域.

3. 设 D 为一主理想整环, F 为 D 的商域. 证明: F 内任一包含 D 的子环 D' 仍为主理想整环 (域看作主理想整环), 而且 D' 是 D 关于某一乘性子集的分式环. 反之, D 的任一分式环是 F 的一个子环, 因而仍是主理想整环.

4. 设 m 是一个无平方因子的整数且 $m \neq 0, 1$. 令 $F = \mathbf{Q}(\sqrt{m}) = \{a + b\sqrt{m} \mid a, b \in \mathbf{Q}\}$, 则 F 是一个域, 叫做有理数域 $\mathbf{Q}$ 上的二次域. F 中有一个子环 R 定义如下:

当 $m \equiv 2$ 或 $3 \pmod 4$ 时, $\quad R = \{a + b\sqrt{m} \mid a, b \in \mathbf{Z}\}$,

当 $m \equiv 1 \pmod 4$ 时, $\quad R = \{a + b \cdot \dfrac{1+\sqrt{m}}{2} \mid a, b \in \mathbf{Z}\}$.

证明 R 是 F 的一个子环. R 以后分别记作 $\mathbf{Z}[\sqrt{m}]$, $\mathbf{Z}[\frac{1+\sqrt{m}}{2}]$(即 §2 中的 R_m). R 叫做 F 的代数整数环.

5. 假设 $\mathbf{Q}(\sqrt{m}), \mathbf{Z}[\sqrt{m}]$ 或 $\mathbf{Z}[\frac{1}{2}(1+\sqrt{m})]$ 如习题 4. $\mathbf{Z}[\sqrt{m}]$ 或 $\mathbf{Z}[\frac{1}{2}(1+\sqrt{m})]$ 统记作 R_m. R_m 的单位乘法群记作 R_m^*. 证明:

(i) $R_{-1}^* = \{\pm 1, \pm\sqrt{-1}\}$;

(ii) $R_{-3}^* = \{\pm 1, \pm\omega, \pm\omega^2\}$, 其中 $\omega = \frac{1}{2}(-1+\sqrt{-3})$, ω 是一个本原三次单位根;

(iii) 当 $m < 0$ 但 $m \neq -1, -3$ 时, $R_m^* = \{\pm 1\}$.

6. 设 H 为四元数体. 令 $D = \{a_0 + a_1 I + a_2 J + a_3 K \mid a_0, \cdots, a_3$ 或全为整数或全为奇整数的一半 $\}$. 证明: D 是 H 的一个子环, 并确定 D 的单位群.

7. 设 H, D 如题 6. 证明 D 的每个理想是一个主理想.

8. 证明: 域 F 上一元形式幂级数环 $F[[x]]$ 是一个主理想整环, 而且 $F[[x]]$ 只有一个非零的素理想 (x), 因而它也是唯一的极大理想. 试问 $F[[x]]$ 的其它理想取什么形式?

9. 证明 $\mathbf{Z}[x]$ 的任一个主理想非极大.

10. 证明 $\mathbf{Z}[\sqrt{-5}]$ 满足因子链条件. 进一步证明, 习题 5 中的环 R_m 都满足因子链条件.

11. 设 F 为一域, $\mathbf{Q}^+$ 表示非负有理数全体. $\mathbf{Q}^+$ 是一个加法幺半群 (也是乘法幺半群). 用 D 表示下列一元多项式的全体

$$a_1x^{\alpha_1}+a_2x^{\alpha_2}+\cdots+a_nx^{\alpha_n},$$

其中 $a_1,\cdots,a_n\in F$ 而 x 的次数 $\alpha_1,\cdots,\alpha_n$ 允许取 $\mathbf{Q}^+$ 的任意数, 即允许取任意非负有理数. 这样两个多项式相等规定为同类单项式的系数一一相等; 它们相加规定为同类单项式的系数一一相加; 它们相乘规定为: 先按分配律展开, 然后单项式相乘

$$a_ix^{\alpha_i}\cdot b_jx^{\beta_j}=a_ib_jx^{\alpha_i+\beta_j},$$

最后按加法求和. 证明 D 构成一个整环, 并且 D 不满足因子链条件.

12. 证明 $\mathbf{Z}[\frac{1}{2}(1+\sqrt{5})]$ 为欧几里得整环.

13. 设 D 为一欧几里得整环, 证明, 若 D 的 d 函数满足

(i) $d(a\cdot b)=d(a)\cdot d(b)$;

(ii) $d(a+b)\leq\max[d(a),d(b)]$;

则 D 是一个域或者是域上一元多项式环.

14. 设 p 为一奇素数. 证明: 在整数环 $\mathbf{Z}$ 内 $x^2\equiv -1\ (\mathrm{mod}\ p)$ 有解的充要条件是 $p\equiv 1\ (\mathrm{mod}\ 4)$.

15. 设 R_m 为习题 5 所定义的. R_m 的元素 π 是一个不可约元的充要条件是范数 $N(\pi)$ 是 $\mathbf{Z}$ 的一个素数.

16. 设 p 为一素数. 证明:

(i) 若 $p\equiv 1\ (\mathrm{mod}\ 4)$, 则 p 在高斯整数环 $R_{-1}=\mathbf{Z}[\sqrt{-1}]$ 内可分解成两个共轭的不可约元的乘积. 由此证明, 若 $p\equiv 1\ (\mathrm{mod}\ 4)$, 则 p 可表成两个有理数的平方和.

(ii) 若 $p\equiv -1\ (\mathrm{mod}\ 4)$, 则 p 也是 R_{-1} 的不可约元.

(iii) 2 在 R_{-1} 内与一个不可约元的平方相伴, 即

$$2=(1+\sqrt{-1})(1-\sqrt{-1})=-\sqrt{-1}(1+\sqrt{-1})^2,$$

其中 $1+\sqrt{-1}$ 是不可约元.

17. 根据习题 16 定出高斯整数环 $\mathbf{Z}[\sqrt{-1}]$ 的全部不可约元.

18. 证明: 一个正整数 m 可以表成两个整数的平方和, 其充要条件是在 m 的标准分解式中出现的 $4k+3$ 形式的素数的幂指数为偶数.

19. 设 R 为一个有 1 的交换环, P 为它的一个素理想. 在多项式环 $R[x_1,\cdots,x_n]$ 中, 如果一个多项式 $f(x_1,\cdots,x_n)$(假设同类项都已合并) 的系数在 R 内生成的理想与 P 互素, 则 $f(x_1,\cdots,x_n)$ 叫做关于 P 的**本原多项式**. 证明, 两个关于 P 的本原多项式的乘积仍是关于 P 的本原多项式.

20. 设 R 为一个唯一因子分解整环, S 是由 R 的一些不可约元生成的半群. 证明, 分式环 $S^{-1}R$ 仍为一个唯一因子分解整环.

21. 证明 $f(x)=x^{p-1}+x^{p-2}+\cdots+1$ 在 $\mathbf{Z}[x]$ 内不可约, 其中 p 为素数.

22. 判定下列多项式在高斯整数环 $R_{-1}=\mathbf{Z}[\sqrt{-1}]$ 上是否可约?

(i) $f(x)=x^{p-1}+x^{p-2}+\cdots+x+1$, p 为素数;

(ii) $f(x)=x^4+(8+\mathrm{i})x^3+(3-4\mathrm{i})x+5, \mathrm{i}=\sqrt{-1}$.

23. 设 D 为一主理想整环. 证明: 若 D 不是域, 则 $D[x]$ 不是主理想整环.

24. 证明: 主理想整环的商环的每个理想仍为主理想.

25. 在 $R_{10}=\mathbf{Z}[\sqrt{10}]$ 中证明:

(i) $\varepsilon=\sqrt{10}+3$ 是一个单位.

(ii) R_{10} 的任一个单位 u 可写成 $u=\pm\varepsilon^r, r\in\mathbf{Z}$. 因此 R_{10} 的单位群 U 等于一个 2 阶群 $\langle -1\rangle$ 和一个无限循环群 $\langle\varepsilon\rangle$ 的直积. $\pm\varepsilon^{\pm 1}$ 叫做 R_{10} 的基本单位. (注意, 若 $v=a+b\sqrt{10}$ 是 R_{10} 的单位, 则 $\pm v^{\pm 1}=\pm a\pm b\sqrt{10}$ 也都是 R_{10} 的单位.)

(iii) R_{10} 不是唯一因子分解整环.

26. 设 p 为一素数, S 表示与 p 互素的整数全体. 则 S 为 $\mathbf{Z}$ 的一个乘性子集. 作 $\mathbf{Z}$ 对 S 的分式环 $S^{-1}\mathbf{Z}$, 记作 $\mathbf{Z}_S$. 证明:

(i) 决定 $\mathbf{Z}_S$ 的单位群 U;

(ii) 证明 $P=\mathbf{Z}_S\setminus U$ 是 $\mathbf{Z}_S$ 的唯一极大理想;

(iii) $\mathbf{Z}_S$ 的每个非零理想是 P 的一个方幂.

27. 设 S 为交换环 R 的一个子环而且 S 与 R 有相同的单位元素. 证明: R 的任一个素理想 P 与 S 的交 $P\cap S$ 是 S 的一个素理想. 问 R 的任一极大理想 M 与 S 的交 $M\cap S$ 是不是 S 的极大理想?

28. 在 $R_2=\mathbf{Z}[\sqrt{2}]$ 中, 证明:

(i) $\varepsilon=1+\sqrt{2}$ 是一个单位.

(ii) R_2 的每个单位 u 可表成 $u=\pm\varepsilon^r, r\in\mathbf{Z}$. 因而 $\pm\varepsilon^{\pm 1}$ 是基本单位而且 R_2 的单位群 $U=\langle -1\rangle\times\langle\varepsilon\rangle$.

29. 在第 4 题的假设下, 证明:

(i) 当 $m\equiv 2$ 或 $3 \pmod 4$ 时, $(R_m=\mathbf{Z}[\sqrt{m}])$, $\sqrt{m}$ 的极小多项式 $=x^2-m$;

(ii) 当 $m\equiv 1 \pmod 4$ 时, $(R_m=\mathbf{Z}[\frac{1}{2}(1+\sqrt{m})])$, $\frac{1}{2}(1+\sqrt{m})$ 的极小多项式为 $x^2-x+\frac{1}{4}(1-m)$.

30. 承上题. 设 P 为 R_m 的一个非零素理想. 证明:

(i) 交 $P\cap\mathbf{Z}$ 是 $\mathbf{Z}$ 的一个非零素理想. 因而 $P\cap\mathbf{Z}=p\mathbf{Z}$, p 是含于 P 内的唯一的素数.

(ii) 商环 $F=R_m/P$ 是一个整环而且包含 $\mathbf{F}_p=\mathbf{Z}/p\mathbf{Z}$ 作为子域.

(iii) $F=\mathbf{F}_p[\alpha]$, α 表示陪集 $\sqrt{m}+P$ 或陪集 $\frac{1}{2}(1+\sqrt{m})+P$ 按照 $m\equiv 2$ 或 $3 \pmod 4$ 或 $m\equiv 1 \pmod 4$ 而定. 而且 α 在 $\mathbf{F}_p$ 上的极小多项式是 $x^2-m \pmod P$ 的因式, 或是

$x^2-x+\frac{1}{4}(1-m) \pmod P$ 的因式按上述两种情况而定. 总之 F 是 p 个元素或 p^2 个元素的有限整环, 因而 F 是一个域. 由此可知. R_m 的任一非零素理想是极大理想.

31. 承 29 题. 设 p 为一素数, p 在 R_m 内生成的理想记作 R_mp, 证明:

(i) $R_mp\cap\mathbf{Z}=\mathbf{Z}p$, 而且商环 $R=R_m/R_mp$ 包含 $\mathbf{F}_p=\mathbf{Z}/\mathbf{Z}p$ 作为子域.

(ii) $R=\mathbf{F}_p[\gamma]$, γ 表示陪集 $\sqrt{m}+R_mp$ 或陪集 $\frac{1}{2}(1+\sqrt{m})+R_mp$ 按照 $m\equiv 2$ 或 $3 \pmod 4$ 或 $m\equiv 1 \pmod 4$ 而定. 而且按照这两种情况, γ 的极小多项式是 $x^2-m \pmod{\mathbf{Z}p}$ 或 $x^2-x+\frac{1}{4}(1-m) \pmod{\mathbf{Z}p}$. 总之, R 是含 p^2 个元素的有限环.

(iii) 设 $x^2-m \pmod{\mathbf{Z}p}$ 可约. 若

$$x^2-m\equiv(x-a)(x-b) \pmod{\mathbf{Z}p},$$

其中 $a,b\in\mathbf{Z}$ 而且 $a\not\equiv b \pmod{\mathbf{Z}p}$, 则 R_m 的理想

$$P_1=(p,\sqrt{m}-a),\quad P_2=(p,\sqrt{m}-b)$$

是素理想. 而且

$$R_mp=P_1\cap P_2=P_1\cdot P_2.$$

(iv) 设 $x^2-m \pmod{\mathbf{Z}p}$ 可约. 若

$$x^2-m\equiv(x-a)^2 \pmod{\mathbf{Z}p},\quad a\in\mathbf{Z},$$

则 R_m 的理想 $P=(p,\sqrt{m}-a)$ 是素理想. 而且

$$R_mp=P^2.$$

这种情况仅当 $p=2$ 或 $p|m$ 时才能出现.

(v) 若 $x^2-m \pmod{\mathbf{Z}p}$ 不可约, 则 R_mp 是 R_m 的素理想.

(vi) 在情况 (iii)–(v) 中用 $x^2-x+\frac{1}{4}(1-m)$ 替代 x^2-m, 结论仍然成立. 此时 (iv) 仅当 $p|m$ 时才能出现.

因此, 明显地决定了 R_m 的一切素理想.

32. 承 29 题. 证明:

(i) 设 d 为任一正整数, 则商环 R_m/R_md 是含 d^2 个元素的有限环.

(ii) 设 A 为 R_m 的任一非零理想, 则交 $A\cap\mathbf{Z}$ 是 $\mathbf{Z}$ 的一个非零理想. 令 $A\cap\mathbf{Z}=\mathbf{Z}d$, 则商环 R_m/A 的元素的个数不超过 d^2.

(iii) R_m 是一个诺特环.

33. 证明:

(i) 诺特环的商环为诺特环;

(ii) 有限多个诺特环的直和为诺特环;

(iii) 诺特环的分式环为诺特环;

(iv) 举例说明, 诺特环的子环不必是诺特环.

34. 一个唯一因子分解整环 R 模它的一个非零素理想得到的商环不必是唯一因子分解整环.

35. 唯一因子分解整环的子环不必是唯一因子分解整环.

36. 诺特环的诣零根 N 是幂零的, 即存在一个正整数 r 使得 $N^r = (0)$.

37. 设 R 为一诺特环. 证明, R 上形式幂级数环 $R[[x]]$ 也是诺特环.

第五章　模

这一章讨论一个环上的模. 模简单说来就是一个与环有着密切联系的交换群. 初看起来，交换群、域上的线性空间以及环本身在结构上有许多差异，但是它们都可以统一在模这个概念下，详细说明将在下面给出. 先在这里指出它们一个共同点，就是它们都是交换群，其自同态分别和整数环、域 (域也是环) 相联系. 我们首先来研究交换群的自同态.

§1　交换群的自同态环

设 M 为一个交换群, 运算写成 "+". 我们已经知道 M 的全部自同构组成一个乘法群, M 的全部自同态, 记作 $\operatorname{End} M$, 组成一个乘法幺半群. 设 $\eta, \zeta \in \operatorname{End} M$, 积 $\eta \cdot \zeta$ 规定为

$$(\eta \cdot \zeta)(x) = \eta(\zeta(x)),\quad x \in M.$$

由于 M 的运算交换，还可以对 $\operatorname{End} M$ 定义加法，和 $\eta + \zeta$ 规定如下

$$(\eta + \zeta)(x) = \eta(x) + \zeta(x),\quad x \in M.$$

首先要验证的是 $\eta + \zeta$ 是不是 M 的一个自同态. 一方面由定义

$$\begin{aligned}(\eta + \zeta)(x + y) &= \eta(x + y) + \zeta(x + y)\\ &= \eta(x) + \eta(y) + \zeta(x) + \zeta(y).\end{aligned}$$

另一方面，由定义，

$$(\eta + \zeta)(x) + (\eta + \zeta)(y) = \eta(x) + \zeta(x) + \eta(y) + \zeta(y).$$

由于 M 的运算交换，所以

$$(\eta + \zeta)(x + y) = (\eta + \zeta)(x) + (\eta + \zeta)(y).$$

因而 $\eta + \zeta$ 是 M 的一个自同态.

$\operatorname{End} M$ 对加法构成一个加法交换群是明显的. 零同态 $0(x) = 0, x \in M$, 是 $\operatorname{End} M$ 的零元素， η 的负元素是 $-\eta$, 规定为

$$(-\eta)(x) = -\eta(x).$$

End M 对加法和乘法构成一个有单位元素的环. M 的恒等同构 $1(x)=x$, 是 End M 的单位元素. 最后只需验证分配律. 设 $\eta,\zeta,\xi\in \operatorname{End} M$.

$$\begin{aligned}(\xi(\eta+\zeta))(x)&=\xi((\eta+\zeta)(x))=\xi(\eta(x)+\zeta(x))\\&=\xi(\eta(x))+\xi(\zeta(x))\\&=(\xi\eta)(x)+(\xi\zeta)(x)\\&=(\xi\eta+\xi\zeta)(x).\end{aligned}$$

所以

$$\xi(\eta+\zeta)=\xi\eta+\xi\zeta.$$

另一个分配律, 读者自己验证. End M 叫做交换群 M 的 **自同态环**.

例 1 设 M 为一无限循环群 $\langle a\rangle$. 运算加法. 设 $\eta\in \operatorname{End} M$. 令 $\eta(a)=za, z\in \mathbf{Z}$. 则 $\eta(na)=nza$. 因而 η 由 a 的象唯一决定. η 可记作 η_z. 反之, 每一个整数 z 决定 M 的一个自同态 η_z. 对于 $z_1, z_2\in\mathbf{Z}$. 有

$$\begin{aligned}(\eta_{z_1}+\eta_{z_2})(a)&=\eta_{z_1}(a)+\eta_{z_2}(a)=z_1a+z_2a\\&=(z_1+z_2)(a)=\eta_{z_1+z_2}(a).\end{aligned}$$

而且

$$(\eta_{z_1}\cdot\eta_{z_2})(a)=\eta_{z_1}(\eta_{z_2}(a))=z_1z_2a=\eta_{z_1\cdot z_2}(a).$$

所以 $z\mapsto\eta_z$ 是 $\mathbf{Z}$ 到 End M 的一个环同态, 由上可知是满同态. 显然这个同态是单一的, 所以

$$\operatorname{End} M\cong\mathbf{Z}.$$

例 2 设 M_n 为一个 n 阶加法循环群 $\langle a\rangle$. 仿上可以建立 $\mathbf{Z}$ 到 End M_n 的一个满同态 $z\mapsto\eta_z$ 使得 $\eta_z(a)=za$. 此时同态的核不再是 (0) 而是 (n), 所以

$$\operatorname{End} M_n\cong\mathbf{Z}/(n).$$

例 3 设 R 为一个幺环. R 作为一个加法群, 它的自同态环记作 End$(R,+)$. 对于每个 $a\in R$, 映射 $x\mapsto ax$, $x\in R$, 是加法群 R 的一个自同态, 记作 a_l, a_l 叫做 R 的一个 **左乘**. 于是 $a_l(x)=ax$. 对 $a,b\in R$, 有

$$\begin{aligned}(a_l+b_l)(x)&=a_l(x)+b_l(x)=ax+bx\\&=(a+b)x=(a+b)_l(x),\\(a_l\cdot b_l)(x)&=a_l(b_l(x))=a(bx)=abx\\&=(ab)_l(x).\end{aligned}$$

这样 End$(R,+)$ 的一个子集 $R_l=\{a_l\,|\,a\in R\}$ 构成一个子环，与 R 成同态. 而且若 $a\neq b$, 则 $a_l(1)=a\neq b=b_l(1)$. 所以 $a_l\neq b_l$. 因而 $a\mapsto a_l$ 是 R 到 R_l 的同构.

对于每个 $a\in R$, 定义加法群 R 的一个自同态 a_r 如下：

$$a_r(x)=xa.$$

a_r 叫做 R 的一个 **右乘**. 同样对于 $a,b\in R$ 有

$$a_r+b_r=(a+b)_r.$$

但是

$$\begin{aligned}(a_r\cdot b_r)(x)&=a_r(b_r(x))=a_r(xb)\\&=xba=(ba)_r(x).\end{aligned}$$

令 $R_r=\{a_r\,|\,a\in R\}$. R_r 是 End$(R,+)$ 的一个子环，与 R 成反同构. $a\mapsto a_r$ 是 R 到 R_r 的一个反同构.

§2 环上的模

设 R 为一个幺环， M 为一个交换加法群. 如在第二章中一个群作用在一个集合上一样，将环 R 作用在交换群 M 上，要求这种作用既反映环的运算也反映群的运算. 这样就形成了模的概念，详细地说

定义 1 设 R 为一个幺环， M 为一个交换群. 若存在 $R\times M$ 到 M 的一个映射 $(a,x)\mapsto ax$ 满足下列条件：

1) $a(x+y)=ax+ay$, $a\in R$, $x,y\in M$;

2) $(a+b)x=ax+bx$, $a,b\in R$, $x\in M$;

3) $(ab)x=a(bx)$;

4) $1\cdot x=x$;

则 M 叫做环 R 上的一个 **左模** 或叫做一个 **左 R- 模**.

若固定元素 a, 则映射按照 1), 确定 M 的一个自同态 $x\mapsto ax$. 这个自同态记作 η_a, $\eta_a(x)=ax$. 于是 $a\mapsto\eta_a$ 是 R 到 End M 的一个映射. 根据 2) 和 3), 这个映射是 R 到 End M 的一个同态，而且根据 4), 将 R 的单位元素映射到 End M 的单位元素. 总之， M 是一个左 R- 模，即是说将 R 的元素从左边作用于 M 引起 R 到 End M 的一个环同态，而且保持单位元素映到恒等自同构.

同样，若存在一个 $M\times R$ 到 M 的映射 $(x,a)\mapsto xa$ 满足

1′) $(x+y)a=xa+ya$, $a\in R$, $x,y\in M$;

2') $x(a+b)=xa+xb,\ a,b\in R,\ x\in M$;

3') $x(ab)=(xa)b$;

4') $x\cdot 1=x$;

则 M 叫做环 R 上的一个 **右 R- 模**.

注意 设 M 是一个右 R- 模, 设 R' 是一个与 R 成反同构的环, 则 M 可以如下看作一个左 R'- 模. 设 $a\mapsto a'$ 是 R 到 R' 的一个反同构. 规定 R' 在 M 上的作用如下

$$a'x=xa.$$

则 M 就是一个左 R'- 模. 当 R 为一个交换环时, 左 R- 模和右 R- 模一致.

例 1 设 $R=F$ 为一个域, $M=V$ 为 F 上一个线性空间. R 在 M 上的作用现在就是 F 的元素对 V 中向量作数乘. 于是 V 就是一个左 F- 模. 因为 F 乘法交换, V 同时也是一个右 F- 模.

例 2 设 $R=\mathbf{Z}$ 为整数环, $M=G$ 为一个交换群, 运算为乘法. 对 $n\in\mathbf{Z},a\in G$, 规定

$$na=a^n,$$

则 G 就是一个左 $\mathbf{Z}$- 模. 若 G 的运算为加法, 则 $\mathbf{Z}$ 在 G 上的作用和 G 的运算在形式上没有区别, 若 $n>0$, 则 $n\cdot a=na=a+\cdots+a(n$ 次).

例 3 设 R 为一个幺环. 把 R 看作加法群, 暂时记作 R_+. 若规定 R 对 R_+ 的作用如下: $a\in R,x\in R_+$, 规定

$$ax=a_l(x),$$

则 R_+ 是一个左 R- 模, 若规定 R 对 R_+ 作用为

$$xa=a_r(x),$$

则 R_+ 是一个右 R- 模.

例 4 设 V 为域 F 上一个线性空间. $\boldsymbol{A}$ 为 V 的任意给定的线性变换. 令 $R=F[\lambda]$ 为 F 上的一元多项式环, λ 为 F 上的未定元. $M=V$. 定义 $F[\lambda]$ 在 V 上的作用如下: 对 $f(\lambda)\in F[\lambda],\alpha\in V$, 规定

$$f(\lambda)\cdot\alpha=f(\boldsymbol{A})(\alpha),$$

则 V 是一个左 $F[\lambda]$- 模. 这个模的结构完全由给定的线性变换 $\boldsymbol{A}$ 决定. $f(\lambda)$ 对向量 α 的作用详细写出就是: 设 $f(\lambda)=a_0+a_1\lambda+\cdots+a_n\lambda^n$, $a_i\in F$, 则 $f(\boldsymbol{A})=a_0\boldsymbol{E}+a_1\boldsymbol{A}+\cdots+a_n\boldsymbol{A}^n$. $\boldsymbol{E}$ 为单位变换,

$$f(\lambda)\cdot\alpha=f(\boldsymbol{A})(\alpha)=a_0\alpha+a_1\boldsymbol{A}(\alpha)+\cdots+a_n\boldsymbol{A}^n(\alpha).$$

§3 关于模的一些基本概念和结果

以后谈到模，R- 模都是指左 R- 模，而关于右 R- 模的结果完全和左 R- 模的结果平行.

设 R 为一个幺环，M 为一个 R- 模，于是从定义推得：

$$a\cdot 0=0,\ a(-x)=-a\cdot x,\ \ a\in R, x\in M.$$
$$0\cdot x=0,\ (-a)x=-a\cdot x.$$
$$a\cdot\sum_{i=1}^{v}x_i=\sum_{i=1}^{v}a\cdot x_i,\quad \left(\sum_{i=1}^{v}a_i\right)\cdot x=\sum_{i=1}^{v}a_i\cdot x.$$

定义 2 M 的一个非空子集 N 叫做 M 的一个 **子模**，若 N 满足：

1) N 为 M 的一个子群；

2) 对 $a\in R, y\in N$ 恒有 $ay\in N$.

$\{0\}$ 和 M 本身显然都是 M 的子模，叫做 M 的 **平凡子模**. 就 §2 中的四个例子来看一下它们的子模.

例 1 V 中的线性子空间和子模的概念一致．V 的每个线性子空间是一个子模；反之，V 的每个子模是一个线性子空间.

例 2 交换群 G 的每个子群 H 是 $\mathbf{Z}$- 模 G 的一个子模，因为对 $n\in\mathbf{Z}, x\in H, nx=x^n\in H$.

例 3 环 R 的每个左理想是模 R 的一个子模；反之，模 R 的每个子模是环 R 的一个左理想，若 R 是一个右 R- 模，则环 R 的右理想和模 R 的子模概念一致.

例 4 设 V_1 是 $F[\lambda]$- 模 V 的一个子模，则对 $f(\lambda)\in F[\lambda], \alpha\in V_1, f(\lambda)\cdot\alpha\in V_1$. 首先，因为 $F\subset F[\lambda]$, V_1 是 V 的一个线性子空间. 特别取 $f(\lambda)=\lambda, \lambda\alpha=\boldsymbol{A}(\alpha)\in V_1$, V_1 是线性变换 $\boldsymbol{A}$ 的一个不变子空间．反之，$\boldsymbol{A}$ 的每一个不变子空间显然是 V 的一个子模.

模 M 的任意多个子模的交仍为一个子模，子模 $N_1,\cdots,N_r$ 的和是指下列元素的集合

$$a_1x_1+\cdots+a_rx_r,\ \ x_i\in N_i,\ \ a_i\in R.$$

这个集合仍是 M 的一个子模，记作 $N_1+\cdots+N_r$. 特别，在 M 中取定 r 个元素 $y_1,\cdots,y_r$. 令 $N=\{\sum a_iy_i\,|\,a_i\in R\}$, 则 N 是 M 的一个子模，叫做由 $y_1,\cdots,y_r$**生成的子模**. N 可记作 $N=Ry_1+\cdots+Ry_r$.

定义 3 设 N 为 R- 模 M 的一个子模．首先，N 作为 M 的一个子群，是 M 的正规子群．作商群 $\overline{M}=M/N$, 仍是一个交换群．在自然的方式下规定 R

在 $\overline{M}$ 上的作用. 设 $a\in R,\overline{x}\in\overline{M},x\in M$ 为 $\overline{x}$ 的任一代表, 规定

$$a\overline{x}=a(x+N)=ax+N.$$

这个定义与 $\overline{x}$ 的代表的取法无关. 设 y 为 $\overline{x}$ 的任一代表, 则 $y-x=z\in N$. $ay-ax=a(y-x)=az\in N$. 因而 $ay+N=ax+N$. 不难验证此作用满足模的定义中的四个条件. 于是 $\overline{M}$ 成为一个 R- 模, 叫做模 M 对子模 N 的 **商模**.

在上面例 3 中, 设 N 为环 R 的一个左理想, 则商群 R/N 是一个 R- 模. 在例 4 中, 设 V_1 为 V 的一个 $\boldsymbol{A}$ 的不变子空间, 则商空间 V/V_1 是一个 $F[\lambda]$- 模, $\boldsymbol{A}$ 在商模 V/V_1 中引起一个线性变换.

定义 4 设 M 和 M' 为两个 R- 模, 若存在 M 到 M' 的一个映射 η 满足:

1) η 是一个群同态;

2) $\eta(ax)=a\eta(x)$, $a\in R$, $x\in M$.

则 η 叫做 M 到 M' 的一个 **模同态** 或 **R-同态**. 若 η 是 M 到 M' 的一个一一对应, 则 η 叫做一个 **模同构**.

设 N 为 R- 模 M 的一个子模. 我们知道, 映射 $\nu:x\mapsto x+N$ 是群 M 到商群 $\overline{M}=M/N$ 的自然同态. 对模来说, ν 还是模 M 到商模 $\overline{M}$ 的一个模同态, 这是因为 $\nu(a\cdot x)=ax+N=a(x+N)=a\nu(x)$.

考虑 M 到 M' 的一个模同态 η. η 的同态象 $\eta(M)$ 是 M' 的一个子模, 这是因为对 $a\in R,x\in M$ 有 $a\eta(x)=\eta(ax)\in\eta(M)$. 其次, 核 $\ker(\eta)$ 是 M 的一个子模, 这是因为对 $x\in\ker(\eta),a\in R$ 有 $\eta(ax)=a\eta(x)=a\cdot 0=0$, 所以 $ax\in\ker(\eta)$. 和群的同态基本定理平行的有

模同态基本定理 设 η 为 R- 模 M 到 R- 模 M' 的一个模同态, 则 $\ker(\eta)$ 和 $\eta(M)$ 分别是 M 和 M' 的子模. 而且 η 诱导出模同构 $\overline{\eta}:M/N\to\eta(M),N=\ker(\eta)$, 使得

$$\overline{\eta}(x+N)=\eta(x),\quad x\in M.\quad\square$$

这里只需验证群同构 $\overline{\eta}$ 是一个模同构.

和群的同态定理平行的有

定理 1 设 η 是 R- 模 M 到 R- 模 M' 的一个满同态, 则 η 诱导出 M 的包含 $\ker(\eta)$ 的全部子模组成的集合 S 和 M' 的全部子模组成的集合 S' 之间的一个一一对应 $H\mapsto\eta(H),H\in S$, 使得

$$\eta^{-1}(\eta(H))=H,\quad H\in S,$$
$$\eta(\eta^{-1}(H'))=H',\quad H'\in S'.\quad\square$$

定理 2 设 η 为 R- 模 M 到 R- 模 M' 的一个模同态, H 为 M 的任一包含 $N=\ker(\eta)$ 的子模, 则 η 诱导出模同构 $\overline{\eta}: M/H \to \eta(M)/\eta(H)$ 使得

$$\overline{\eta}(x+H)=\eta(x)+\eta(H),\ x\in M.$$

若将 $\eta(M)$ 与 M/N 等同: $\eta(x)=x+N$, 则得

$$M/H \cong (M/N)/(H/N). \quad \square$$

定理 3 设 H,N 为 R- 模 M 的两个子模, 则

$$H+N/N \cong H/H\cap N.$$

而且映射 $x+N \mapsto x+(H\cap N)$ 是一个模同构. $\square$

证明和群的相应定理一样, 在这里只需验证定理中出现的群同构保持环在模上的作用.

定义 5 设 M 为一个 R- 模. 若存在一个 $x\in M$ 使得 $M=Rx$, 即 M 的元素 y 都可表成 $y=ax$, $a\in R$, 则 M 叫做一个 **循环 R- 模**.

一个循环群 (a) 就是一个循环 $\mathbf{Z}$- 模.

一个幺环 R 看成一个 R- 模, 它也是一个循环 R- 模, 因为 $R=R\cdot 1$.

定义 6 设 M 为一个 R- 模, $x\in M$. 由 x 生成的子模 Rx 本身就是一个循环 R- 模. 首先 R 和 Rx 作为加法群, 有一个群同态

$$\zeta_x : a \mapsto ax,\ \ a\in R,$$

而且它还是模 R 到模 Rx 的一个模同态, 因为对 $b\in R$,

$$b(\zeta_x(a))=b(a\cdot x)=(ba)\cdot x=\zeta_x(ba).$$

$\ker(\zeta_x)$ 是 R 中一个左理想, $\ker(\zeta_x)=\{a\in R\,|\,a\cdot x=0\}$. 因此, $\ker(\zeta_x)$ 叫做元素 x 的 **零化子** 或 x 在 R 中的零化子, 记成 $\ker(\zeta_x)=\mathrm{ann}(x)$. 于是

$$Rx \cong R/\mathrm{ann}(x)$$

成模同构. 若 $\mathrm{ann}(x)=\{0\}$, 则 $Rx\cong R, ax=0 \iff a=0$. $\mathrm{ann}(x)$ 也叫做 x 的 **阶理想**. 当 R 交换时, $\mathrm{ann}(x)$ 是 R 的一个 (双边) 理想.

我们来定义模的零化子. 设 M 为一个 R- 模. 规定

$$\mathrm{ann}(M)=\{a\in R\,|\,a\cdot x=0\text{对所有}x\in M\}.$$

显然 ann(M) 是一个左理想，同时它也是一个右理想. 因为，对于任意 $a \in$ ann(M), $b \in R$, $x \in M$, 有 $bx \in M$, 因而 $(ab)x = a(bx) = 0$. ann(M) 叫做 M 的 **零化子**. 显然有

$$\mathrm{ann}(M) = \bigcap_{x \in M} \mathrm{ann}(x).$$

除零模外，R 的单位元素 1 不属于 ann(M).

设 M 为一个 R- 模，$M \neq (0)$, I 为 M 的零因子. 若元素 b, c 属于同一个剩余类 $a - I$, 则 $bx = cx$ 对所有 $x \in M$. 因此 M 可以看作一个 R/I- 模，若规定 $\bar{a} = a + I$ 对 M 的作用如下：

$$\bar{a}x = ax, \quad x \in M.$$

例 1 设 G 为一个交换群. $x \in G$, G 作为 $\mathbf{Z}$- 模，x 的零化子 ann(x) 为 $\mathbf{Z}$ 的一个理想，令 ann$(x) = (n)$, 于是 $\langle x \rangle \cong \mathbf{Z}/(n)$. 当 $n = 0$ 时，$\langle x \rangle \cong \mathbf{Z}$, $\langle x \rangle$ 是一个无限循环群. 当 $n > 0$ 时，$\langle x \rangle$ 为一个 n 阶循环群，n 为 x 的阶，(n) 为 x 的阶理想.

例 2 设 V 为域 F 上一个 n 维线性空间，$\boldsymbol{A}$ 为一个线性变换. 如前，V 是一个 $F[\lambda]$- 模. $\lambda x = \boldsymbol{A}(x)$. $x \in V$. 对一个固定的 x, x 生成一个循环 $F[\lambda]$- 子模 $V_1 = F[\lambda]x$, ann(x) 是 $F[\lambda]$ 的一个理想. ann$(x) = (m(\lambda))$. $m(\lambda)$ 的首项系数取作 1,$m(\lambda)$ 由 x 唯一决定，叫做 x 的 **极小多项式**. 由 ann(x) 的定义可知 $f(\lambda)x = 0 \iff m(\lambda)|f(\lambda)$. 设 $m(\lambda) = a_0 + a_1\lambda + \cdots + a_{m-1}x^{m-1} + x^m$, 则向量 $x, \lambda x, \cdots, \lambda^m x$ 在 F 上线性相关，但是 $x, \lambda x, \cdots, \lambda^{m-1}x$ 则线性无关，不难看出 m 是向量组 $x, \lambda x, \lambda^2 x, \cdots$ 的秩. 若 $x \neq 0$, 则 $m > 0$, $m(\lambda)$ 是一个正次数多项式；若 $x = 0$, 则 $m(\lambda) = 1$, ann$(0) = F[\lambda]$.

仿照 §1, 考虑一个 R- 模 M 的全部 R- 自同态构成的集合 $\mathrm{End}_R M$, 其中不仅有乘法而且还可以定义加法，两个 R- 自同态的和仍为一 R- 自同态，$\mathrm{End}_R M$ 对加法和乘法构成一个有单位元素的环，叫做模 M 的 **自同态环**.

例 1 域 F 上的线性空间 V, V 是一个 F- 模. V 的每个 F- 自同态 η 是一个线性变换，反之也对. 所以 V 的自同态环就是由全部线性变换组成的环.

例 2 一个交换群 G 作为 $\mathbf{Z}$- 模的自同态环就是群 G 的自同态环.

例 3 设 V 为一个 $F[\lambda]$- 模，$\lambda x = \boldsymbol{A}(x)$. V 的每个 $F[\lambda]$ 自同态 η 首先是一个 F- 自同态. 因而是 V 作为 F 上线性空间的一个线性变换. 其次 $\eta(\lambda x) = \lambda\eta(x)$ 对 $x \in V$, 即 $\eta\boldsymbol{A} = \boldsymbol{A}\eta$. 因而 η 是与 $\boldsymbol{A}$ 乘法交换的线性变换. 反之，与 $\boldsymbol{A}$ 交换的 V 的线性变换当然是一个 $F[\lambda]$- 自同态.

例 4 设 R 为一个幺环，R 看作左 R- 模，设 η 为模 R 的一个 R- 自同态. 令 $\eta(1) = b_\eta$. 于是对 $x \in R$, $\eta(x) = \eta(x \cdot 1) = x\eta(1) = xb_\eta$, 所以 $\eta = (b_\eta)_r$ 是用

b_r 对 R 作右乘得到的右乘变换. 反之，每个右乘变换 b_r 是一个 R- 自同态，因为 $b_r(ax) = (ax)b = a(xb) = ab_r(x)$. 所以 R 作为左 R- 模，它的自同态环等于 R 的右乘变换环 R_r.

§4 自由模

设 R 为一个幺环，M 为一个 R- 模，设 S 为 M 的任一非空子集. 下列所有有限和

$$\sum_{x\in S} a_x x, \quad a_x \in R,$$

其中只有有限多个 a_x 不为 0, 在 M 中组成的子集显然构成 M 的一个子模，它叫做由 S **生成的子模**, S 叫做这子模的一组 **生成元**. M 本身恒有一组生成元，例如 $M^* = M - \{0\}$ 就是. M 的任一有限子集 $S_1 = \{x_1, \cdots, x_r\}$ 称为 R-**线性无关的**, 如果从任一线性关系

$$a_1x_1 + \cdots + a_rx_r = 0, \quad a_i \in R,$$

恒推出 $a_1 = \cdots = a_r = 0$. M 的任一非空子集 S 叫做 R-**线性无关的**, 如果 S 的任一有限子集是 R- 线性无关的. M 的一组生成元 S 叫做 M 的一 **基**, 如果 S 是 R- 线性无关的. 设 S 是 M 的一基，则 M 的每个元素表成上面的有限和，其表法是唯一的，就是说，若有两个有限和相等

$$\sum_{x\in S} a_x x = \sum_{x\in S} b_x x,$$

则 $a_x = b_x$, 对所有 $x \in S$.

若 M 有一组由有限多个元素组成的生成元，则 M 叫做 **有限生成的**. 在这一章里我们只讨论有限生成的 R- 模.

定义 7 若 R 模 M 有一基，则 M 叫做一个 **自由** R- **模**.

一个模总是可以找到一组生成元，但不一定有基. 例如有限交换群作为一个 $\mathbf{Z}$- 模，则不是自由模，下面利用 R 的集合积作出自由模.

令 $R^{(n)}$ 表示 n 个 R 的集合积 $R \times R \times \cdots \times R$, $n \geq 1$. $R^{(n)}$ 中元素记为 $(x_i) = (x_1, x_2, \cdots, x_n), (y_i)$ 等. 规定 $R^{(n)}$ 的加法和 R 对 $R^{(n)}$ 的作用如下

$$\begin{aligned}
&(x_1, x_2, \cdots, x_n) + (y_1, y_2, \cdots, y_n) \\
&\quad = (x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n), \\
&a \cdot (x_1, x_2, \cdots, x_n) = (ax_1, ax_2, \cdots, ax_n), \ a \in R.
\end{aligned}$$

不难验证 $R^{(n)}$ 是一个 R- 模，零元素 $(0,0,\cdots,0)$ 记作 0，(x_i) 的负元为 $-(x_i)=(-x_i)$. 令

$$
\begin{aligned}
e_1 &= (1,0,\cdots,0),\\
e_2 &= (0,1,\cdots,0),\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
e_n &= (0,0,\cdots,1),
\end{aligned}
$$

则 $R^{(n)}$ 的元素 (x_i) 可表成

$$(x_i)=x_1e_1+x_2e_2+\cdots+x_ne_n.$$

而且因为 $(x_i)=0$ 推出 $x_1=\cdots=x_n=0, e_1,\cdots,e_n$ 是 R- 线性无关的. 所以 $e_1,\cdots,e_n$ 是 $R^{(n)}$ 的一基，$R^{(n)}$ 是一个自由 R- 模. 若 R 为一域，则 $R^{(n)}$ 就是 n 维线性空间.

定理 4 设 M 为一个自由 R- 模，$u_1,\cdots,u_n$ 为它的一基. 设 M' 为任一个 R- 模，$v_1,\cdots,v_n$ 为 M' 的任一个子集，于是映射 $u_i\mapsto v_i$ 恒可唯一地扩充成 M 到 M' 的一个 R- 同态.

证明 作 M 到 M' 的映射

$$\sum_{i=1}^{n}a_iu_i\mapsto\sum_{i=1}^{n}a_iv_i,\quad a_i\in R,$$

这是 M 到 M' 的一个模同态，因为，首先象由原象唯一确定，即若 $\sum a_iu_i=\sum b_iu_i$，则 $a_i=b_i$，$i=1,\cdots,n$，于是 $\sum a_iv_i=\sum b_iv_i$. 至于映射保持运算，由验算即得. 显然这个映射由 u_i 的象唯一确定. □

定理 4 是自由模的一个特征的刻画. 这里虽然限制在有限生成的自由模，其实定理 4 对任意自由模成立. 以下两个命题也是如此.

推论 设 M 为一个以元素 $u_1,\cdots,u_n$ 为基的自由模，则 $M\cong R^{(n)}$.

证明 因为 $u_1,\cdots,u_n$ 为 M 的一基，映射

$$\sum a_iu_i\mapsto\sum a_ie_i$$

为 M 到 $R^{(n)}$ 的一个模同态，又因 $e_1,\cdots,e_n$ 为 $R^{(n)}$ 的一基，因而逆映射

$$\sum a_ie_i\mapsto\sum a_iu_i$$

为 $R^{(n)}$ 到 M 的一个模同态，所以 $M\cong R^{(n)}$. □

设 R 为一个幺环，M 为一个 R- 模，S 为 M 的一组生成元，I 为 R 的一个理想. 所有有限和

$$a_1x_1+a_2x_2+\cdots+a_rx_r,\quad a_i\in I,\quad x_i\in S,$$

构成的集合记作 IS. 显然 IS 是 M 的一个子模 IS 与 M 的生成元集选取无关. 设 S' 为 M 的任一生成元集, 求证 $IS = IS'$. S' 的每个元 y 可表成

$$y = b_1x_1 + b_2x_2 + \cdots + b_sx_s, \quad b_i \in R, x_i \in S.$$

用 I 的元素 a 作用得

$$ay = ab_1x_1 + ab_2x_2 + \cdots + ab_sx_s,$$

由于 I 是 R 的理想, $ab_i \in I$, $i = 1, \cdots, s$. 从而 $ay \in IS$. 由此可知 $IS' \subset IS$. 同理 $IS \subset IS'$. 所以 $IS = IS'$.

引理 设 M 为一个自由的 R- 模, $x_1, \cdots, x_r$ 为它的一基, I 为 R 的一个理想. 令 $N = Ix_1 + \cdots + Ix_r$, 则商模 M/N 可看作 $\overline{R} = R/I$- 模, 而且 M/N 是 $\overline{R}$ 上的一个自由模, $\overline{x}_i = x_i + N$ $(i = 1, \cdots, r)$ 是它的一基.

证明 首先我们知道 $\overline{M} = M/N$ 是一个 R- 模, 而且 $\overline{x}_i = x_i + N$, $i = 1, \cdots, r$ 是它的一组生成元. 对于任一元素 $\overline{x} \in \overline{M}$, $\overline{x}$ 可表成 $\overline{x} = a_1\overline{x}_1 + \cdots + a_r\overline{x}_r$, 根据 R 对 $\overline{M}$ 的作用有

$$\overline{x} = a_1\overline{x}_1 + \cdots + a_r\overline{x}_r = \overline{a_1x_1} + \cdots + \overline{a_rx_r} = \overline{a_1x_1 + \cdots + a_rx_r},$$

由此可知 $\overline{x} = 0$ 当且仅当 $a_1x_1 + \cdots + a_rx_r \in N$. 由于 $x_1, \cdots, x_r$ 是 M 的一基, 根据 N 的定义可知 $a_1x_1 + \cdots + a_rx_r \in N$ 当且仅当所有 $a_i \in I$. 由此可知, I 是 $\overline{M}$ 的零化子. 因而 $\overline{M}$ 可看作一个 $\overline{R}$- 模. 在这种看法下, $\overline{x} = \overline{a}_1\overline{x}_1 + \cdots + \overline{a}_r\overline{x}_r$, $\overline{a}_i = a_i + I$. 由上可知, $\overline{x} = 0$ 当且仅当所有 $\overline{a}_i = 0$. 所以 $\overline{x}_1, \cdots, \overline{x}_r$ 为 $\overline{M}$ 的一基, $\overline{M}$ 是一个自由的 $\overline{R}$- 模. □

定理 5 设 R 为一个交换幺环, M 为一个自由 R- 模. 则 M 的任意两基有相同的基数.

证明 设 $x_1, \cdots, x_r$ 和 $y_1, \cdots, y_s$ 为 M 的两基. 由于 R 有单位元素而且交换, R 有极大理想. 设 I 为 R 的一个极大理想. 根据引理前的说明, $N = Ix_1 + \cdots + Ix_r = Iy_1 + \cdots + Iy_s$. 令 $\overline{R} = R/I$. 根据引理, 商模 $\overline{M} = M/N$ 是 $\overline{R}$ 上的自由模, $\overline{x}_1, \cdots, \overline{x}_r$ 和 $\overline{y}_1, \cdots, \overline{y}_s$ 是它的两基. 由于 I 为极大理想, $\overline{R}$ 为一个域, 因而 $\overline{M}$ 为域 $\overline{R}$ 上的线性空间. 它的维数等于任一基所含元素的个数. 所以 $\overline{M}$ 的维数 $= r = s$. □

设 R 为一个交换幺环. 一个自由 R- 模 M 的基所含元素的个数是自由模 M 的一个不变量, 它叫做自由模 M 的**秩**. 零模看作自由模, 它的秩为 0.

推论 设 R 为一个交换幺环. 若 $R^{(m)}$ 和 $R^{(n)}$ 成模同构, 则 $m = n$.

证明 由定理 5 和定理 4 的推论即得. □

环上的自由模是域上线性空间的一种推广.

例 1 设 $R=\mathbf{Z}/(6)$. $R^{(2)}$ 是一个秩为 2 的自由 R- 模, $e_1=(\overline{1},\overline{0})$ 和 $e_2=(\overline{0},\overline{1})$ 是 $R^{(2)}$ 的一基. $R^{(2)}$ 中每个非零元素并不都是 R- 线性无关的. 例如 $x=\overline{2}e_1+\overline{3}e_2$ 是 R- 线性无关的, 而 $y=\overline{2}e_1+\overline{2}e_2$ 则在 R 上是线性相关的, 因为 $\overline{3}\cdot y=0$.

例 2 设 $R=\mathbf{Z}, M=\mathbf{Z}^{(2)}$, $e_1=(1,0), e_2=(0,1)$ 为 M 的一基. 由 $x_1=2e_1$ 和 $x_2=3e_2$ 在 M 中生成的子模 N 是 M 的一个真子模. 而且 N 还是 R 上的自由模, x_1,x_2 是 N 的一基, 因而 N 和 M 有相同的秩.

例 3 设 $R, M=R^{(2)}$ 如例 1,$y=\overline{2}e_1+\overline{2}e_2$ 在 M 中生成的子模 N 由元素 $0, y, 2y$ 组成. N 不再是自由 R- 模. 因而自由模的子模不必是自由模.

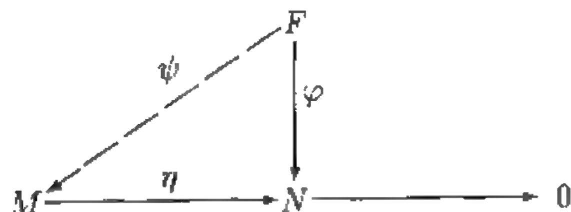
以上例子说明, 环上的自由模和域上的线性空间有许多不同的性质.

自由 R- 模还有一个很好的性质. 它是从定理 4 引伸出来的.

定理 6 设 F 为一个自由 R- 模, M,N 为两个任意 R- 模而且 $\eta: M\to N$ 是任意一个满同态. 于是 F 到 N 的任一个模同态 φ 恒可提升为 F 到 M 的一个模同态 ψ 使得

$$\eta\cdot\psi=\varphi.$$

如图



其中横行 $M\to N\to 0$ 表示 η 是满射.

证明 设 $S=\{u_\lambda\,|\,\lambda\in I\}$ 为 F 的一基, 其中 I 为指标集. 由于 η 是满射, 因而每个 $\varphi(u_\lambda)$ 在 η 下有原象. 对于任一 λ, 取定一个 $x_\lambda\in M$ 使得

$$\eta(x_\lambda)=\varphi(u_\lambda),\quad \lambda\subset I.$$

于是, 根据定理 4, 存在一个唯一的模同态 $\psi: F\to M$ 使得

$$\psi(u_\lambda)=x_\lambda,\quad \lambda\in I.$$

由验算,

$$\eta\cdot\psi(u_\lambda)=\eta(\psi(u_\lambda))=\eta(x_\lambda)=\varphi(u_\lambda),\quad \lambda\in I.$$

$\eta\cdot\psi$ 和 φ 在 F 的一基 S 上作用相等, 因而 $\eta\cdot\psi=\varphi$. □

推论 设 $\eta: M \to N$ 是一个满的模同态. 若 N 是一个自由模, 则存在 M 的一个子模 L 使得 $M = \ker\eta \oplus L$.

证明 在定理 6 中令 $F = N, \varphi = 1_N$. 然后取 $L = \mathrm{Im}\psi$. 由 η 的满性, $M = \ker\eta + L$. 由 $\eta\psi = 1_N, \ker\eta \cap L = (0)$. □

根据上面的讨论, 给定一个交换幺环 R 和一个正整数 n, 存在一个而且只有一个 (在模同构意义下) 秩为 n 的自由 R- 模, 秩不相同的自由 R- 模互相不能模同构. 后面这句话对几类重要的非交换环也是对的.

最后来考虑交换环上自由模的自同态环. 设 R 为一个交换幺环, M 为一个自由 R- 模. 设 σ 是 M 的一个模自同态, 取定 M 的一基 $e_1, \cdots, e_n$. M 的任一个元素 x 可唯一表成 $x = x_1e_1 + \cdots + x_ne_n$, 于是

$$\begin{aligned}\sigma(x) &= \sigma(x_1e_1) + \cdots + \sigma(x_ne_n)\\ &= x_1\sigma(e_1) + \cdots + x_n\sigma(e_n).\end{aligned} \tag{1}$$

σ 由基在 σ 下的象唯一决定, 将 $\sigma(e_i)$ 表成

$$\sigma(e_i) = \sum_{j=1}^{n} a_{ji}e_j, \quad i = 1, \cdots, n. \tag{2}$$

这样 M 的每个模自同态 σ 确定了 R 上的一个 $n \times n$ 矩阵 $A = (a_{ij})$. 由于 R 是交换环, 左 R- 模也是一个右 R- 模. $x \cdot a = a \cdot x$, $a \in R, x \in M$. 于是 (2) 可用矩阵的形式表出.

$$\sigma(e_1, \cdots, e_n) = (e_1, \cdots, e_n)A. \tag{3}$$

反之, 任给一个 $n \times n$ 矩阵 $A = (a_{ij})$, $a_{ij} \in R$, 由 (1) 和 (2) 定义 M 到自身的一个映射 σ, 这个映射显然是 M 的一个模自同态. 用 $M_n(R)$ 表示元素属于 R 的 $n \times n$ 矩阵的全体. 于是在 $\mathrm{End}M$ 和 $M_n(R)$ 之间建立了一个一一对应 $\sigma \to A$. σ 和 A 的对应关系由 (3) 确定, 而 (2) 又是通过 M 的基 $e_1, \cdots, e_n$ 表示出来的. 因此, A 叫做 **自同态 σ 在基 $e_1, \cdots, e_n$ 下的矩阵**.

我们想通过上述一一对应来定义 $M_n(R)$ 中的运算, 设 σ, τ 为 M 的任意两个模同态, 在基 $e_1, \cdots, e_n$ 下的矩阵分别为 A 和 B. 令 $\sigma + \tau$ 和 $\sigma \cdot \tau$ 在基 $e_1, \cdots, e_n$ 下的矩阵分别为 C 和 D. 于是把 C 和 D 分别叫做矩阵 A 和 B 的和与积, 记成 $C = A + B, D = A \cdot B$. 通过 (2) 式实际计算发现, C 的 (i,j) 位置的元素等于 A, B 的同位置的元素的和, D 的 (i,j) 位置的元素等于 A 的第 i 行和 B 的第 j 列对应元素乘积的和, 这就是高等代数中见到的矩阵的加法和乘法. 这样, 一一对应 $\sigma \to A$ 保持加法和乘法, 自同态 $\mathrm{End}M$ 的一切运算规律当然在 $M_n(R)$ 中也成立, 于是 $M_n(R)$ 构成一个环, 而且与 $\mathrm{End}M$ 成环同构.

在上述同构映射下 End$M$ 的单位元素和 $M_n(R)$ 的单位元素即单位矩阵 E 相对应.

M 的模自同构全体记作 Aut$M$. $M_n(R)$ 的可逆矩阵全体记作 $GL_n(R)$. 上述环同构诱导出 End$M$ 的单位群 Aut$M$ 和 $M_n(R)$ 的单位群 $GL_n(G)$ 的同构.

在高等代数课程里介绍过的关于数域上 $n\times n$ 矩阵的行列式理论完全可以移植到交换环 R 上 $n\times n$ 矩阵环 $M_n(R)$ 中来, 那里的行列式的基本性质在这里都保持成立. 有一点需要指出的是关于逆矩阵的问题. 由于环 R 中一个非零元素不必有逆, $M_n(R)$ 的矩阵 A, 虽然它的行列式 $|A|$ 不等于零, A 不必有逆. 容易证明, A 有逆的充要条件是 A 的行列式 $|A|$ 在 R 内是一个单位. 也会出现这样的情形, 虽然两个矩阵 A 与 B 的行列式都不等于零, 它们的乘积 AB 的行列式可能等于零.

§5 模的直和

对一个模进行分解的时候, 必然会遇到模的直和这个概念.

定义 8 设 $M_1,\cdots,M_r$ 为同一个环 R 上的模. 首先作加法群 $M_1,\cdots,M_r$ 的直和 $M=M_1\oplus\cdots\oplus M_r$, 然后规定 R 对 M 的作用如下:

$$a(x_1,\cdots,x_n)=(ax_1,\cdots,ax_r),$$

对于 $(x_1,\cdots,x_r)\in M, a\in R$, 则 M 成为一个 R- 模. M 叫做 R- 模 $M_1,\cdots,M_r$ 的 **直和**. M 可简记作 $\bigoplus\limits_{1}^{r} M_i$.

与群的直和一样, 模的直和 $M=\bigoplus\limits_{1}^{r} M_i$ 包含 r 个子模 M_i', 它由下列元素组成

$$x_i'=(0,\cdots,0,x_i,0,\cdots,0),\quad x_i\in M_i,\ i=1,\cdots,r.$$

而且 M_i' 和 M_i 成模同构, 同构由映射 $x_i\mapsto(0,\cdots,0,x_i,0,\cdots,0)$ 给出.

下列定理刻画了模直和的特征.

定理 7 *设 M 和 N 为两个 R- 模, 而且 M 是 r 个 R- 模 $M_1,\cdots,M_r$ 的直和. 如果存在 M 的子模 M_i' 到 N 的模同态 ψ_i $(i=1,\cdots,r)$, 则 $\psi_1,\cdots,\psi_r$ 可以唯一地开拓成模同态 $\psi: M\to N$, 使得 ψ 满足 $\psi(x_i')=\psi_i(x_i')$, $i=1,\cdots,r$.*

证明 如果 ψ 存在, 则 $\psi(x_1,\cdots,x_r)=\psi(x_1'+\cdots+x_r')=\psi(x_1')+\cdots+\psi(x_r')=\psi_1(x_1')+\cdots+\psi_r(x_r')$. 因而 ψ 由 ψ_i 唯一决定. 其次证明 ψ 存在. 我们定义 ψ 如下:

$$\psi(x_1,\cdots,x_r)=\psi_1(x_1')+\cdots+\psi_r(x_r'),\quad (x_1,\cdots,x_r)\in M.$$

证明 ψ 是一个模同态.

$$\begin{aligned}\psi((x_i)+(y_i)) &= \psi((x_i+y_i))\\ &= \psi_1(x_1'+y_1')+\cdots+\psi_r(x_r'+y_r'),\\ \psi((x_i))+\psi((y_i)) &= \psi_1(x_1')+\cdots+\psi_r(x_r')+\\ &\quad \psi_1(y_1')+\cdots+\psi_r(y_r')\end{aligned}$$

由于 N 是交换群, 因而 $\psi((x_i)+(y_i))=\psi((x_i))+\psi((y_i))$. $\psi(a(x_i))=a\psi((x_i))$ 是显然的. 所以 ψ 是一个模同态. 由 ψ 的定义可知 $\psi(x_i')=\psi_i(x_i')$, $i=1,\cdots,r$. □

设 $M=\bigoplus_1^r M_i$ 为 R- 模直和, 它的子模 M_i' 如上. 和群的直和一样, M_i' 满足

1) $M=M_1'+\cdots+M_r'$;

2) $M_i'\cap(M_1'+\cdots+\hat{M}_i'+\cdots+M_r')=\{0\}$, $i=1,\cdots,r$.

而且有下面的

定理 8 设 N 为一个 R- 模且包含 r 个子模 M_i, 满足:

1) $N=M_1+\cdots+M_r$;

2) $M_i\cap(M_1+\cdots+\hat{M}_i+\cdots+M_r)=\{0\}$, $i=1,\cdots,r$;

则存在模同构 $\psi: M=\bigoplus_1^r M_i\to N$ 使得

$$\psi((x_1,\cdots,x_r))=x_1+\cdots+x_r,\ (x_1,\cdots,x_r)\in M.\quad □$$

如果 R- 模 N 的 r 个子模 $M_1,\cdots,M_r$ 满足定理 8 中条件 2), 则 $M_1,\cdots,M_r$ 叫做**独立的**. 若 N 的子模 $M_1,\cdots,M_r$ 是独立的, 则从等式 $x_1+\cdots+x_r=0$, $x_i\in M_i, i=1,\cdots,r$, 恒可推出 $x_1=\cdots=x_r=0$.

如果 R- 模 N 的 r 个子模 $M_1,\cdots,M_r$ 满足定理 8 中条件 1) 和 2), 则 N 叫做子模 M_i 的**内直和**. 仍记作 $N=M_1\oplus\cdots\oplus M_r$. 根据定理 8, 直和与内直和在模同构意义下没有区别.

为了下一章的应用, 把几个简单的结果集中写成一个定理.

定理 9

1) 若 R- 模 M 是子模 $M_1,\cdots,M_r$ 的直和, 而且每个 M_i 又是子模 $M_{i1},\cdots,M_{in_i}$ 的直和, 则 M 是子模 M_{ij} $(j=1,\cdots,n_i, i=1,\cdots,r)$ 的直和.

2) 若 R- 模 M 是子模 $N_1,N_2,\cdots,N_r$ 的直和. 令 $M_1=N_1+\cdots+N_{s_1}, M_2=N_{s_1+1}+\cdots+N_{s_2},\cdots,M_t=N_{s_{t-1}+1}+\cdots+N_r$, 则 M 是 $M_1,M_2,\cdots,M_t$ 的直和.

3) 若 R- 模 M 是子模 $M_1, \cdots, M_r$ 的直和. 令 $N = M_1 + \cdots + M_s$, $1 \le s < r$, 则商模 M/N 和 $M_{s+1} + \cdots + M_r$ 成模同构. □

习 题

(以下恒假定 R 是幺环)

1. 设 M 是一个左 R- 模, η 是环 S 到 R 的一个同态, 而且 η 将 S 的单位元素映到 R 的单位元素. 我们定义 S 在 M 上的作用如下: 对于 $a \in S, x \in M$, 规定

$$ax = \eta(a)(x).$$

证明 M 是一个 S- 模.

2. (见 §1 零化子的定义) 设 M 是一个左 R- 模, $B = \{b \in R \mid bx = 0 \text{对所有的} x \in M\}$. 证明: B 是 R 的一个理想, 而且对于包含在 B 中的 R 的任一个理想 I, 可以定义商环 R/I 在 M 上的作用如下使得 M 成为一个 R/I- 模:

$$(a + I)x = ax, \quad a \in R, x \in M.$$

3. 设 M 和 M' 是两个左 $\mathbf{Z}$- 模. 证明: 若 M 和 M' 是加法群同构的, 则 M 和 M' 也是 $\mathbf{Z}$- 模同构的. 更精确地说, 若 η 是 M 到 M' 的一个加法群同构, 则 η 也是一个 $\mathbf{Z}$- 模同构.

4. 设 $\mathbf{Q}$ 为有理数域, M 和 M' 是两个左 $\mathbf{Q}$- 模. 证明: 若 $\eta: M \to M'$ 是一个加法群同构, 则 η 也是一个 $\mathbf{Q}$- 模同构. (* 如果用实数域 $\mathbf{R}$ 替代 $\mathbf{Q}$, 问这个命题是否成立?)

5. 设 M 是一个有限交换群而且 $M \neq 0$. 问 M 是否能成为一个左 $\mathbf{Q}$- 模.

6. 设 M, N 为两个 R- 模, 用 $\mathrm{Hom}_R(M, N)$ 表示 M 到 N 的 R- 同态的全体. 它对同态的加法成一交换群. 若 $R = \mathbf{Z}$, $\mathrm{Hom}_{\mathbf{Z}}(M, N)$ 可简记成 $\mathrm{Hom}(M, N)$. 证明: $\mathrm{Hom}(\mathbf{Z}, \mathbf{Z}/(n)) \cong \mathbf{Z}/(n)$, $\mathrm{Hom}(\mathbf{Z}/(n), \mathbf{Z}) \cong 0$.

7. 设 M 为一个 R- 模.

(i) 规定 R 对 $\mathrm{Hom}_R(R, M)$ 的作用如下: 对 $f \in \mathrm{Hom}_R(R, M)$, $a \in R$, 规定 $a \cdot f$ 为

$$af(r) = f(ra), \quad r \in R.$$

证明 $\mathrm{Hom}_R(R, M)$ 是一个 R- 模.

(ii) 设映射 $\eta: \mathrm{Hom}_R(R, M) \to M$; $\eta(f) = f(1), f \in \mathrm{Hom}_R(R, M)$. 证明 η 是一个 R- 同构.

8. 设 M 为一个左 R- 模. 对每个 $a \in R$, a 决定 M 的一个群同态 σ_a 使得 $\sigma_a(x) = ax, x \in M$. 令 $S = \{\sigma_a \mid a \in R\}$. 证明: S 在 M 的自同态环 $\mathrm{Hom}(M, M)$ 中的中心化子是 M 的 R- 自同态环 $\mathrm{Hom}_R(M, M)$, 其中 S 的中心化子定义为 $\{\sigma \in \mathrm{Hom}(M, M) \mid \sigma\sigma_a = \sigma_a\sigma \text{对所有} a \in R\}$.

9. M, σ_a 定义如习题 8, 问在什么条件下 σ_a 属于 $\mathrm{Hom}_R(M, M)$?

10. 如果一个非零 R- 模 M 除 $\{0\}$ 和 M 外无其它子模, 则 M 叫做**不可约**的. 不可约模也叫**单模**. 证明: R- 模 M 是不可约的当且仅当 M 是一个非零循环模, 而且每个非零元都是它的生成元.

11. 幺环 R 的一个左 (右) 理想 I 叫做极大的, 若 $I \neq R$ 而且不存在左 (右) 理想 I' 使得 $I \subsetneq I' \subsetneq R$. 证明: 左 R 模 M 是不可约的当而且仅当存在 R 的一个极大左理想 I, 使得 M 和 R- 模 R/I 成模同构.

12. (舒尔 (Schur) 引理) 证明:

(i) 若 M_1, M_2 是不可约 R- 模, 则 M_1 到 M_2 的模同态不是零同态便是模同构.

(ii) 一个不可约模的模自同态环 $\mathrm{End}_R(M)$ 即 $\mathrm{Hom}_R(M, M)$ 是一个体.

13. 承上题, 若 $\mathrm{End}_R M$ 是一个体, 问 M 是否必须是不可约的?

14. 设 R 为一个交换环, η 是 $R^{(n)}$ 的一个 R- 自同态. 证明: 若 η 是满的, 则 η 是单一的, 因而 η 是一个 R- 自同构. 反之, 设 η 是单一的, 问 η 是否是满的?

15. 设 M, N 为两个左 R- 模. 定义 R 在 $\mathrm{Hom}(M, N)$ 上的作用如下: 对于 $a \in R, \sigma \in \mathrm{Hom}(M, N)$, 规定

$$(a\sigma)(x) = a(\sigma(x)), \quad x \in M.$$

证明 $\mathrm{Hom}(M, N)$ 是一个左 R- 模. 试问 $\mathrm{Hom}_R(M, N)$ 是不是 $\mathrm{Hom}(M, N)$ 的子模?

16. 在习题15 中令 $M = R^{(m)}, N = R^{(n)}$, 而且假定 R 为交换环. 证明 $\mathrm{Hom}(R^{(m)}, R^{(n)})$ 为一个自由 R- 模, 而且秩 $= m \cdot n$.

17. 设 M_i, $i = 1, \cdots, r$ 为 R- 模 M 的子模. 若 M_i 满足

(i) $M = M_1 + \cdots + M_r$;

(ii) $(M_1 + \cdots + M_i) \cap M_{i+1} = (0)$, $i = 1, 2, \cdots, r-1$;

则 $M = M_1 \oplus \cdots \oplus M_r$.

18. 设 R 为一交换环, 自由模 $R^{(n)}$ 的一基为 $e_1, \cdots, e_n$. 令 $f_i = \sum_{j=1}^{n} a_{ij} e_j$, $i = 1, \cdots, n$, $A = (a_{ij}) \in M_n(R)$, 证明:

*(i) $f_1, \cdots, f_n$ 在 R 上线性无关的充要条件是 A 的行列式 $\det A \neq 0$, 而且不是 R 的零因子.

(ii) 设 A 满足 (i) 中条件, 于是 $f_1, \cdots, f_n$ 在 $R^{(n)}$ 内生成一个自由子模 N, $f_1, \cdots, f_n$ 是它的一基. 作商模 $M = R^{(n)}/N$. 求证 M 的零化子包含主理想 $(|A|)$, $|A| = \det A$. 因而 M 可看成一个 $R/(|A|)$- 模.

19. 将 $\mathbf{Z}/(n)$ 看作 $\mathbf{Z}$- 模. 问下列模是否可写成两个非零子模的直和:

(i) $\mathbf{Z}/(p^e)$, p 为一素数, $e \geq 1$;

(ii) $\mathbf{Z}/(n)$, $n = p_1^{e_1} \cdots p_r^{e_r}$, $p_1, \cdots, p_r$ 为不同的素数, $e_i \geq 1$, $i = 1, \cdots, r$.

20. 证明: $\mathbf{Q}$ 作为 $\mathbf{Z}$- 模, 它的任一有限生成的子模是循环模. 由此证明, $\mathbf{Q}$ 不是一个自由 $\mathbf{Z}$- 模.

21. 证明: 若 M 是一个自由左 R- 模, $u_1, \cdots, u_n$ 为它的一基, 则 $\mathrm{Hom}_R(M, R)$, 记

作 M^*, 是一个自由右 R- 模, 它有一基 $f_1, \cdots, f_n$ 使得

$$f_i(u_j) = \delta_{ij}, \quad i, j = 1, \cdots, n,$$

δ_{ij} 为克罗内克 (Kronecker) 符号.

22. 设 F 为一个自由 R- 模, P 为 F 的直和项, 即 F 等于子模 P 和 P' 的直和. 又设 M, N 为两个任意的 R- 模, η 为 M 到 N 的一个满同态. 证明: P 到 N 的任一个模同态 φ 恒可提升为 P 到 M 的一个模同态 ψ, 使得 $\eta \cdot \psi = \varphi$.

23. 设 P 为一个 R- 模. 如果对于任意 R- 模 M 和 N 以及任意的满的模同态 $\eta : M \to N$, 任一个模同态 $\varphi : P \to N$ 恒可提升为模同态 $\psi : P \to M$ 使得 $\eta \cdot \psi = \varphi$, 则 P 叫做**投射 R- 模**. 证明: 投射 R- 模必是某个自由 R- 模的直和项. (参看 24 题)

24. 任一 R- 模都是某个自由 R- 模的同态象.

25. 设 $\eta : M \to P$ 是一个 R- 模同态而且是满的. 证明: 若 P 是一个投射模, 则存在一个模同态 $\psi : P \to M$ 使得 $\eta \cdot \psi = 1_P$, 1_P 不是 P 的恒等自同构, 此时 $M = \ker\eta \oplus \mathrm{im}\psi$.

26. 设 P 为一 R- 模, 证明: 如果对于任一 R- 模 M 以及任一满的模同态 $\eta : M \to P$, 恒存在模同态 $\psi : P \to M$ 使得 $\eta \cdot \psi = 1_P$, 则 P 是一个投射模.

27. 证明两个投射 R- 模 P_1 和 P_2 的直和仍为投射模.

28. 证明任一投射 R- 模的直和项仍为投射模.

29. 举一个是投射模但不是自由模的例子.

30. 设 M 为一个有限生成 R- 模, N 为一个子模. 证明: 若 N 是 M 的一个直和项, 则 N 也是有限生成的.

31. 设 N 是环 R 的一个左理想. 证明: 当 R 作为一个左 R- 模时, 子模 N 是 R 的一个直和项的充要条件是 N 作为 R 的子环有右单位元素.

第六章　主理想环上的有限生成模

对于一种代数结构，分类常常是一个基本问题，换句话说，就是要设法刻画出所有可能的互不同构的类型. 当然，在一般的情况下，分类问题不是很容易解决的. 主理想环上的有限生成模的分类可以彻底解决，同时它又包括了不少重要的特例，如有限生成的交换群，又如有限维线性空间中一个线性变换的标准形等. 因之，我们将给出这个问题的全部讨论与最后的结果，然后再看它的两个重要的应用.

在这一章，我们总是假定 R 为一主理想整环，所讨论的模都是 R- 模而且是有限生成的. 为方便起见，以下主理想整环恒简称为主理想环.

§1　主理想环上的自由模

我们首先给出主理想环上有限维自由模的一些基本性质.

定理 1　*设 R 为一主理想环，M 为一自由 R- 模，秩为 n. 于是 M 的任一子模也是自由 R- 模，秩 $\leq n$.*

注意，我们把零模看作秩为 0 的自由模.

证明　设 N 为 M 的一个子模. 如果 M 是一零模，则结论显然. 下面我们对 M 的秩 n 作归纳法. 假设结论对秩小于 n 的自由模已经成立.

令 $\varepsilon_1,\cdots,\varepsilon_n$ 是自由模 M 的一组基. 考虑 N 中一切元素

$$a_1\varepsilon_1+\cdots+a_n\varepsilon_n$$

的第一个系数 a_1 所成的集合 I_1, 显然 I_1 是环 R 的一个理想. 因为 R 是主理想环，所以

$$I_1=(f),$$

其中 $f\in R$. 如果 $f=0$, 即 $I_1=\{0\}$, 这就是说 N 包含在自由模

$$M_1=R\varepsilon_2+\cdots+R\varepsilon_n$$

中，则由归纳法假设，结论成立. 设 $f\neq 0$, 于是在 N 中有一元素

$$h_1=f\varepsilon_1+\cdots$$

对于 N 中任一元素

$$x=a_1\varepsilon_1+\cdots+a_n\varepsilon_n,$$

我们有 $a_1=a_1'f$. 于是

$$x-a_1'h_1\in M_1.$$

令 $N_1 = N \cap M_1$. 上面的讨论表明

$$N = Rh_1 + N_1.$$

显然, $Rh_1 \cap N_1 = \{0\}$. 因之,

$$N = Rh_1 \oplus N_1.$$

由归纳法假设, N_1 是一自由模, 秩 $\leq n-1$.

令 $h_2, \cdots, h_r$ 为 N_1 的一组基, $r \leq n$, 即得

$$N = Rh_1 \oplus Rh_2 \oplus \cdots \oplus Rh_r,$$

这就证明了, $h_1, h_2, \cdots, h_r$ 是 N 的一组基, N 是一自由模, 秩 $= r \leq n$. 由数学归纳法原理, 定理普遍成立. □

推论 主理想环上有限生成模的子模也是有限生成的.

证明 设 M 是主理想环 R 上一有限生成模, $g_1, \cdots, g_m$ 是它的一组生成元. N 是 M 的一个子模. 根据第五章定理 4, 作一秩为 m 的自由模 $R^{(m)}$, 基为 $\varepsilon_1, \cdots, \varepsilon_m$, 有一满同态

$$\eta : R^{(m)} \to M,$$
$$\eta(a_1\varepsilon_1 + \cdots + a_m\varepsilon_m) = a_1g_1 + \cdots + a_mg_m.$$

令 $K = \eta^{-1}(N)$, K 是 $R^{(m)}$ 的一个子模. 由定理 1,K 也是一自由模, 有一组基 $f_1, \cdots, f_r$. 因为 η 是一满同态, 所以

$$h_1 = \eta(f_1), \cdots, h_r = \eta(f_r)$$

是 N 的一组生成元. 这就证明了 N 是有限生成的. □

应该指出, 如果 R 不是主理想环, 那么自由模的子模不一定是自由的. 例如, $R = \mathbf{Z}/6\mathbf{Z}$, R 作为 R- 模是秩为 1 的自由模, $N = 2R$ 就不是自由模. 因为 $2R$ 由 3 个元素组成, 而非零自由模包含元素的个数不少于环 R 元素的个数, 所以 $2R$ 不是自由模.

定义 1 设 M 是一 R- 模. M 中元素 a 称为 **扭元素**, 如果有 $r \in R, r \neq 0$ 使 $ra = 0$. 如果不存在 R 中非零元素 r 使 $ra = 0$, 则 a 称为 **自由的**.

a 是 "自由" 的, 等于说 a 是 R- 线性无关的. R- 线性无关以下简称线性无关.

显然, 当元素 $a \in M$ 是自由的, 由 a 生成的子模 Ra 是秩为 1 的自由模.

例 1 交换群作为 $\mathbf{Z}$- 模, 扭元素就是有限阶元素.

例 2 设 V 是域 F 上的线性空间. V 中每个非零元素都是自由的.

例 3 设 V 是域 F 上一 n 维线性空间, $\boldsymbol{A}$ 是一线性变换. 对于 $\alpha \in V$, 定义 $\lambda \cdot \alpha = \boldsymbol{A}\alpha$, V 可以看作一元多项式环 $F[\lambda]$ 上一个模. 显然, V 作为 $F[\lambda]$-模, 每个元素都是扭元素. (为什么?)

定义 2 设 M 是一 R-模, 如果 M 中每个元素都是扭元素, 则 M 称为**扭模**; 如果 M 中每个非零元素都是自由的, 则 M 称为**无扭模**.

定理 2 主理想环上无扭的有限生成模一定是自由模.

证明 设 M 是主理想环 R 上一无扭的有限生成模, $a_1, \cdots, a_m$ 是 M 的一组生成元.

因为 M 无扭, 所以每个非零元素 c 都线性无关. 由此可知, 只要 M 不是零模, 在这组生成元 $a_1, \cdots, a_m$ 中总可选出一个非空的极大线性无关组, 譬如说, 就是 $a_1, \cdots, a_r$ $(r \leq m)$. 这就是说, $a_1, \cdots, a_r$ 线性无关, 而 $a_1, \cdots, a_r, a_j$ $(r < j \leq m)$ 都线性无关, 即有关系

$$x_{j1}a_1 + \cdots + x_{jr}a_r + x_j a_j = 0, \quad r < j \leq m,$$

其中 $x_j \neq 0$.

如果 M 是零模, 定理自然成立. 因之我们无妨假定 M 不是零模.

由 $a_1, \cdots, a_r$ 的选择, 我们知道 $a_1, \cdots, a_r$ 生成一自由的子模 N, 且 $a_1, \cdots, a_r$ 是 N 的一组基.

令 $x = x_{r+1} \cdots x_m$. 因为 R 是整环, $x \neq 0$. 显然

$$xa_i \in N, \ i = 1, \cdots, m.$$

于是映射

$$a \mapsto xa$$

定义了一个同态

$$\eta : M \to N.$$

M 无扭而且 $x \neq 0$ 保证了同态 η 是单一的, 因之 M 与自由模 N 的子模 $\eta(M)$ 同构. 根据定理 1,M 是自由模. □

在定理 2 中, 有限生成这个条件是重要的. 例如, 有理数 $\mathbf{Q}$ 看作整数环 $\mathbf{Z}$ 上的模是无扭的, 可是任意两个有理数在 $\mathbf{Z}$ 上都是线性相关的, (为什么?) 因之不可能是自由模.

§2 有限生成模的分解 (第一步)

定理 2 表明，如果一有限生成模是无扭的，则是一自由模，而自由模的结构是清楚的，完全被秩所决定. 这一节要讨论一般的情形. 下面将证明，一般的有限生成模的分解可以归结为有限生成的扭模的分解.

设 M 是主理想环 R 上一有限生成模. 我们来证明，M 中全体扭元素组成一子模. 事实上，设 a, b 为 M 中任意两个扭元素，分别有

$$ra = 0 \text{ 与 } sb = 0,$$

其中 $r, s \in R$ 且 $\neq 0$. 显然有 $r \cdot s \neq 0$(因为 R 是整环) 而且

$$rs(a \pm b) = 0,$$

$$r(xa) = 0, \text{ 对于任意 } x \in R.$$

这就是说，M 中全体扭元素对于加、减以及数乘是封闭的，因而全体扭元素成一子模. 我们用 $\mathrm{Tor}(M)$ 表示这个子模.

定理 3 设 M 是主理想环 R 上一有限生成模，于是 $M/\mathrm{Tor}(M)$ 无扭，因而是自由的.

证明 只要证明，$M/\mathrm{Tor}(M)$ 中的扭元素必为零. 令 $a+\mathrm{Tor}(M)$ 为 $M/\mathrm{Tor}(M)$ 中一扭元素，有 $r(a+\mathrm{Tor}(M)) = 0, r \in R, \neq 0$. 由

$$r(a + \mathrm{Tor}(M)) = 0,$$

即得

$$ra \in \mathrm{Tor}(M),$$

于是有 $s \in R$ 且 $s \neq 0$ 使 $s(ra) = (sr)a = 0$ 而且 $sr \neq 0$, 从而 $a \in \mathrm{Tor}(M)$. 这就证明了 $M/\mathrm{Tor}(M)$ 无扭. 显然 $M/\mathrm{Tor}(M)$ 是有限生成的. 由定理 2,$M/\mathrm{Tor}(M)$ 是自由的. □

令

$$M/\mathrm{Tor}(M) \cong F = R^{(t)}$$

是一秩为 t 的自由模. 由自由模的投射性 (第五章定理 6 的推论) 可知，M 中有一子模 K,

$$K \cong R^{(t)}$$

且

$$M = K \oplus \mathrm{Tor}(M).$$

这就证明了

定理 4 主理想环 R 上任一有限生成模 M 都可以分解成它的扭子模 $\mathrm{Tor}(M)$ 与一自由子模 K 的直和， K 的秩是被 M 唯一决定的.

证明 因为 $K \cong M/\mathrm{Tor}(M)$, 所以 K 的秩也就是自由模 $M/\mathrm{Tor}(M)$ 的秩, 当然是被 M 唯一决定的. □

一般说来，自由子模 K 不是唯一决定的，读者不难举出这样的例子.

自由模 $M/\mathrm{Tor}(M)$ 的秩通常就称为**模 M 的秩**.

由定理 4, 有限生成模 M 的分解就归结为它的扭子模 $\mathrm{Tor}(M)$ 的分解. 由定理 1 的推论， $\mathrm{Tor}(M)$ 也是有限生成的. 因之我们下面集中讨论有限生成扭模的情形.

§3 有限生成扭模的分解

设 M 为主理想环 R 上一有限生成的扭模.

对于任意 $a \in R$, 我们定义

$$M(a) = \{x \in M \mid ax = 0\}.$$

显然 $M(a)$ 是一子模.

由定义可知，如果 $a|b$, 则

$$M(a) \subset M(b).$$

如果 a 在 R 中是一单位，则 $M(a) = \{0\}$.

$M(0) = M$ 也是显然的.

设 $a,b \in R, d$ 是 a,b 的一个最大公因子，即 $(d) = (a) + (b)$, 则有

$$M(d) = M(a) \cap M(b).$$

事实上，由 $M(d) \subset M(a), M(d) \subset M(b)$ 即得 $M(d) \subset M(a) \cap M(b)$, 另一方面，设 $x \in M(a) \cap M(b)$. 由 $(d) = (a) + (b)$ 可知，有 $u, v \in R$ 使 $d = ua + vb$, 于是

$$dx = (ua + vb)x = 0,$$

即 $x \in M(d)$. 这就证明了

$$M(d) \supset M(a) \cap M(b).$$

结合以上的讨论即得

$$M(d) = M(a) \cap M(b).$$

根据以上的讨论，我们不难证明

引理 设 $a,b\in R$, $(a,b)=1$, 则

$$M(a)\cap M(b)=\{0\},$$
$$M(ab)=M(a)\oplus M(b).$$

证明 根据上面的讨论，有

$$M(a)\cap M(b)=M((a,b))=M(1)=\{0\}.$$

由 $M(a)\subset M(ab), M(b)\subset M(ab)$, 有

$$M(ab)\supset M(a)+M(b).$$

反过来，如果 $x\in M(ab)$, 即 $abx=0$, 则

$$ax\in M(b),\ bx\in M(a).$$

由 $(a,b)=1$, 有 $u,v\in R$ 使

$$1=ua+vb,$$

于是

$$x=uax+vbx\in M(a)+M(b).$$

这就证明了

$$M(ab)=M(a)+M(b).$$

再由 $M(a)\cap M(b)=\{0\}$, 即得

$$M(ab)=M(a)\oplus M(b).\quad \square$$

定理 5 设 R 为一主理想环，M 为一 R- 模．$a\in R, a\neq 0, a=up_1^{n_1}\cdots p_r^{n_r}$, 其中 u 为一单位，$p_1,\cdots,p_r$ 为互不相伴的素元，$r\geq 1$. 于是有

$$M(a)=\bigoplus_{i=1}^{r}M(p_i^{n_i}).$$

证明 对 r 作归纳法.

当 $r=1$ 时，结论显然.

当 $r>1$, 显然有 $up_1^{n_1}\cdots p_{r-1}^{n_{r-1}}$ 与 $p_r^{n_r}$ 互素，于是应用引理即得

$$M(a)=M(up_1^{n_1}\cdots p_{r-1}^{n_{r-1}})\oplus M(p_r^{n_r}).$$

对 $M(up_1^{n_1}\cdots p_{r-1}^{n_{r-1}})$ 用归纳法假设，我们就得到所要的分解

$$M(a)=\bigoplus_{i=1}^{r}M(p_i^{n_i}).\quad \square$$

证明中，我们用到了一个简单的事实，即当 u 为一单位，$a\in R$, 有

$$M(ua)=M(a).$$

它的证明留给读者.

对于主理想环 R 中任一元素 p, 显然有

$$M(p)\subset M(p^2)\subset\cdots\subset M(p^i)\subset\cdots$$

作它们的并集，

$$\bigcup_{i=1}^{\infty}M(p^i).$$

不难证明，它是 M 的一个子模. 设

$$a,b\in\bigcup_{i=1}^{\infty}M(p^i),$$

这就是说 $a\in M(p^j), b\in M(p^k)$ 对适当的 j,k, 无妨设 $j\le k$. 于是

$$ra\in M(p^j)\subset\bigcup_{i=1}^{\infty}M(p^i),$$
$$a\pm b\in M(p^k)\subset\bigcup_{i=1}^{\infty}M(p^i).$$

定义 3 对于主理想环 R 中任一素元素 p, 子模

$$M_p=\bigcup_{i=1}^{\infty}M(p^i)$$

称为 M 的 p **分量**.

下面重新提一下第五章定义过的一个概念. 设 M 是主理想环 R 上一有限生成模. 对于 M 中元素 a, 子模 N,

$$\mathrm{ann}(a)=\{r\in R\,|\,ra=0\},$$
$$\mathrm{ann}(N)=\{r\in R\,|\,ra=0\ \text{对所有的}\ a\in N\}.$$

分别称为 a 与 N 的零化子.

不难看出， $\mathrm{ann}(a),\mathrm{ann}(N)$ 都是 R 的理想，而且 $\mathrm{ann}(a)=\mathrm{ann}(Ra)$. 证明留给读者.

当然， $\mathrm{ann}(a)$ 与 $\mathrm{ann}(N)$ 可能是零理想. 例如当 a 自由时, 则 $\mathrm{ann}(a)=\{0\}$.

引理 设 M 是主理想环 R 上一有限生成扭模， $a_1,\cdots,a_r$ 是 M 的一组生成元. 于是

1) $\mathrm{ann}(M)=\bigcap_{i=1}^{r}\mathrm{ann}(a_i)$;

2) 存在一非零元素 $x\in R$ 使

$$\mathrm{ann}(M)=(x).$$

证明 请读者证明 1).

2) 因为 $a_1,\cdots,a_r$ 都是扭元素，所以

$$\mathrm{ann}(a_i)=(x_i),\quad x_i\neq 0,\quad i=1,\cdots,r.$$

而 $\bigcap_{i=1}^{r}(x_i)=(x)$, 其中 x 是 $x_1,\cdots,x_r$ 的一个最小公倍. □

定理 6 设 M 是主理想环 R 上一有限生成扭模， $\mathrm{ann}(M)=(x),x=up_1^{n_1}\cdots p_r^{n_r}$, 其中 u 为一单位， $p_1,\cdots,p_r$ 为互不相伴的素元素. 于是有

1) $M=\bigoplus_{i=1}^{r}M(p_i^{n_i})$;

2) 当 p 是一个与 $p_1,\cdots,p_r$ 都不相伴的素元素时， $M_p=\{0\},M_{p_i}=M(p_i^{n_i}),\ i=1,\cdots,r$.

证明 由 $\mathrm{ann}(M)=(x)$ 可知 $M(x)=M$. 应用定理 5 即得 1).

2) 设 p 是一个与 $p_1,\cdots,p_r$ 都不相伴的素元素. 为了证明 $M_p=\{0\}$, 只要证对任一 j,

$$M(p^j)=\{0\}.$$

因为 $(p^j,x)=1$, 所以根据定理 5 前的引理即得

$$\{0\}=M(x)\cap M(p^j)=M\cap M(p^j)=M(p^j).$$

为了证明 $M_{p_i}=M(p_i^{n_i})$. 我们来证，对于任意的 $t\geq n_i$, $M(p_i^t)=M(p_i^{n_i})$. 因为 $(p_i^t,x)=p_i^{n_i}$, 所以我们有

$$M(p_i^t)=M(p_i^t)\cap M=M(p_i^t)\cap M(x)=M(p_i^{n_i}).\quad \square$$

定理 6 说明，任一有限生成的扭模都可以分解成有限多个 p 分量的直和，而定理的 2) 说明这种分解是唯一的.

定义 4 设 M 是主理想环 R 上一有限生成模. 如果 $\mathrm{ann}(M)=(p^n)$, 其中 p 是一素元素，则模 M 称为一 p **模**.

这样，定理 6 就可说成，在主理想环上任一有限生成的扭模都可以分解成一些 p 模的直和. 下面将进一步把 p 模再分解成一些循环的 p 模的直和.

定理 7 *主理想环 R 上任一有限生成的 p 模 M 都可以分解成有限多个循环 p 模的直和.*

证明 设 $a_1,\cdots,a_r$ 是 M 的一组生成元. 我们对生成元的个数 r 作归纳法证明下述结论：主理想环 R 上由 r 个元素生成的 p 模可以分解成不超过 r 个循环 p 模的直和.

当 $r=1$ 时，结论自然成立.

假设结论对生成元的个数 $<r$ 时已经成立，现在来证生成元的个数 $=r$ 的情形.

因为 M 是 p 模，所以有

$$\mathrm{ann}(a_i)=(p^{m_i}),\quad i=1,\cdots,r.$$

在 $m_1,\cdots,m_r$ 中取一最小的，譬如说是 m_r, 即

$$m_i\geq m_r, i=1,\cdots,r-1.$$

令 M_1 为 $a_1,\cdots,a_{r-1}$ 生成的模. 由归纳法假设， M_1 有分解式

$$M_1=N_1\oplus\cdots\oplus N_s,\quad s\leq r-1,$$

其中 $N_i=Rb_i$, $\mathrm{ann}(b_i)=(p^{t_i})$, $i=1,\cdots,s$.

如果 $M_1\cap Ra_r=\{0\}$, 则

$$M=M_1\oplus Ra_r=Rb_1\oplus\cdots\oplus Rb_s\oplus Ra_r,$$

结论成立.

显然 M 可以由 $b_1,\cdots,b_s,a_r$ 生成. 如果 $s<r-1$, 则由归纳法假设，结论成立.

下面看 $s=r-1$ 的情形. 我们指出，在这里无妨假定 $t_i\geq m_r$, $i=1,\cdots,r-1$. 否则，譬如 $t_1<m_r$, 我们就取 b_1 代替原来的 a_r, 考虑 $b_2,\cdots,b_{r-1},a_r$ 生成的子模 M_2, 重复以上的步骤. 经过有限步之后，我们总可以达到 $t_i\geq m_r$, $i=1,\cdots,r-1$ 的情形.

如果 $M_1 \supset Ra_r$ 即 $M_1 = M$, 则结论自然成立.

在一般的情形, 考察商模 M/M_1. 令 $\overline{a}_r$ 为 a_r 在 M/M_1 中的象. 显然 $p^{m_r} \in \operatorname{ann}(\overline{a}_r)$, 从而有

$$\operatorname{ann}(\overline{a}_r) = (p^k), \quad k \leq m_r.$$

由 $p^k\overline{a}_r = 0$, 即 $p^k a_r \in M_1$, 有

$$p^k a_r = x_1 b_1 + \cdots + x_{r-1} b_{r-1}.$$

两边乘以 $p^{m_r - k}$ 得

$$0 = p^{m_r-k} x_1 b_1 + \cdots + p^{m_r-k} x_{r-1} b_{r-1}.$$

由直和分解 $M_1 = N_1 \oplus \cdots \oplus N_{r-1}$ 可知

$$p^{t_i} | p^{m_r-k} x_i, \ i = 1, \cdots, r-1,$$

或者

$$p^{k+t_i-m_r} | x_i, \quad i = 1, \cdots, r-1.$$

由于 $t_i \geq m_r$, $i = 1, \cdots, r-1$, 我们有

$$k + t_i - m_r \geq k, \quad i = 1, \cdots, r-1.$$

因之,

$$p^k | x_i, \quad \text{或者 } x_i = p^k y_i, \quad i = 1, \cdots, r-1.$$

于是

$$p^k a_r = p^k y_1 b_1 + \cdots + p^k y_{r-1} b_{r-1},$$

移项即得

$$p^k (a_r - y_1 b_1 - \cdots - y_{r-1} b_{r-1}) = 0.$$

令

$$b_r = a_r - y_1 b_1 - \cdots - y_{r-1} b_{r-1}.$$

显然 $\overline{b}_r = \overline{a}_r, \operatorname{ann}(\overline{b}_r) \supset \operatorname{ann}(b_r)$. 由此即得

$$\operatorname{ann}(b_r) = (p^k),$$

从而 $M_1 \cap Rb_r = \{0\}$,

$$M = M_1 \oplus Rb_r = Rb_1 \oplus \cdots \oplus Rb_{r-1} \oplus Rb_r.$$

这就是我们要的直和分解，定理得证. □

结合定理 6 与定理 7, 我们得到

定理 8 主理想环 R 上的有限生成扭模 M 可以分解成一些循环 p 模的直和，即

$$M = \bigoplus_{i=1}^{m} N_i, \tag{1}$$

其中 $N_i = Rb_i, \text{ann}(N_i) = \text{ann}(b_i) = (p_i^{n_i}), p_i$ 为 R 中素元素，$i = 1, \cdots, m$. □

分解式涉及到的素元素 $p_1, \cdots, p_m$ 中可能有相伴的，我们知道相伴的元素生成相同的理想，因之我们可以约定相伴的元素都用同一个素元素表示. 重新排列 $N_1, \cdots, N_m$ 的次序，定理中 m 个素元素的方幂 $p_1^{n_1}, \cdots, p_m^{n_m}$ 可以排成：

$$\begin{array}{l} p_1^{n_{11}}, \cdots, p_1^{n_{1r_1}} \\ \cdots\cdots\cdots\cdots\cdots \\ p_s^{n_{s1}}, \cdots, p_s^{n_{sr_s}} \end{array} \tag{2}$$

其中 $p_1, \cdots, p_s$ 是互不相伴的素元素，且

$$n_{i1} \geq n_{i2} \geq \cdots \geq n_{ir_i}, \quad i = 1, \cdots, s.$$

显然，元素组 (2) 在同构的意义下唯一地决定了分解式 (1).

§4 有限生成模的标准分解及其唯一性

结合定理 4 与定理 8, 我们就得到有限生成模的 **第一标准分解**.

定理 9 主理想环 R 上任一有限生成模 M 都可以分解成一自由子模与若干个循环 p 模的直和，即

$$M = K \bigoplus \bigoplus_{i=1}^{s} \bigoplus_{j_i=1}^{r_i} N_{ij_i}, \tag{3}$$

其中 $K \cong R^{(t)}, \text{ann}(N_{ij_i}) = (p_i^{n_{ij_i}}). p_1, \cdots, p_s$ 为互不相伴的素元素，且

$$n_{i1} \geq n_{i2} \geq \cdots \geq n_{ir_i}, \ i = 1, \cdots, s.$$

t 被 M 唯一决定，称为 M 的秩. □

在这个分解式中，属于不同的素元素的循环 p 模可以合并成一些较大的循环模. 为此，我们来证

引理 M 为主理想环 R 上的模， $a,b\in M,\operatorname{ann}(a)=(f),\operatorname{ann}(b)=(g)$. 如果 $(f,g)=1$, 则

$$Ra+Rb=R(a-b),$$

而 $\operatorname{ann}(a+b)=(fg)$.

证明 $R(a+b)\subset Ra+Rb$ 是显然的. 由 $(f,g)=1$, 有 $u,v\in R$ 使 $uf+vg=1$. 于是

$$vg(a+b)=vga=(1-uf)a=a\in R(a+b).$$

同理， $uf(a+b)=b\in R(a+b)$. 这就证明了

$$Ra+Rb\subset R(a+b).$$

因之 $Ra+Rb=R(a+b)$.

令 $\operatorname{ann}(a+b)=(h)$. 显然 $fg\in\operatorname{ann}(a+b)$, 即

$$(fg)\subset(h).$$

反过来，有 $hfb=hf(a+b)=0$, 所以

$$g|hf.$$

由 $(f,g)=1$, 得 $g|h$. 同理， $f|h$. 再根据 $(f,g)=1$, 即得 $fg|h$, 于是

$$(h)=(fg).$$

这就证明了， $\operatorname{ann}(a+b)=(fg)$. □

用引理，由定理 9 不难推出

定理 10 主理想环 R 上任一有限生成模 M 都可以分解成一自由子模与若干个循环模的直和.

$$M=K\bigoplus\bigoplus_{k=1}^{l}M_k \tag{4}$$

其中 $K\cong R^{(t)},\operatorname{ann}(M_k)=(d_k)$, 且

$$d_{k+1}|d_k,\quad k=1,\cdots,l-1.$$

分解式 (4) 称为 **第二标准分解**.

证明 M 有第一标准分解

$$M=K\bigoplus\bigoplus_{i=1}^{s}\bigoplus_{j_i=1}^{r_i}N_{ij_i}.$$

令 $N_{ij_i}=Rb_{ij_i}$, $\text{ann}(b_{ij_i})=\text{ann}(N_{ij_i})=(p_i^{n_{ij_i}})$. 令 $l=\max\limits_i\{r_i\}, c_{ij}=b_{ij_i}$ 当 $j\le r_i$, $c_{ij}=0$, 当 $j>r_i$. $x_k=c_{1k}+c_{2k}+\cdots+c_{sk}$, $k=1,\cdots,l$.

由引理可知

$$Rx_k=Rc_{1k}+Rc_{2k}+\cdots+Rc_{sk},\quad k=1,\cdots,l.$$

且 $\text{ann}(x_k)=(p_1^{n_{1k}}p_2^{n_{2k}}\cdots p_s^{n_{sk}})$, 这里约定 $n_{ik}=0$ 当 $k>r_i$.

令 $Rx_k=M_k$, $\text{ann}(x_k)=(d_k)$. 于是我们有

$$M=K\bigoplus\bigoplus_{k=1}^{l}M_k,$$

且 $d_{k+1}|d_k$, $k=1,\cdots,l-1$. □

显然, 第二标准分解 (4) 是被第一标准分解 (3) 唯一决定. 反过来, 根据定理 5, 由第二标准分解 (4) 立即得到第一标准分解 (3).

下面来讨论标准分解的唯一性问题. 首先我们要说明 "唯一性" 的意义. 在第一标准分解 (3) 中, 子模 N_{ij_i} 一般说来不是唯一决定的, 同样, 在第二标准分解 (4) 中, 子模 M_i 一般也不是唯一决定的. 我们将要证明的是: 在第一标准分解

$$M=K\bigoplus\bigoplus_{i=1}^{s}\bigoplus_{j_i=1}^{r_i}N_{ij_i}$$

中, 自由子模 K 的秩以及 N_{ij_i} 的零化子组

$$\text{ann}(N_{ij_i})=(p_i^{n_{ij_i}}),\ i=1,\cdots,s,\ j_i=1,\cdots,r_i$$

是被 M 唯一决定的. 同样第二标准分解

$$M=K\bigoplus\bigoplus_{k=1}^{l}M_k$$

中, 自由子模 K 的秩与 M_k 的零化子组

$$\text{ann}(M_k)=(d_k),\quad k=1,\cdots,l$$

是被 M 唯一决定.

由于这两个标准分解互相唯一决定, 所以只需要证明其中的一个具有上述的唯一性就行了. 下面就第一标准分解来讨论唯一性. 自由子模 K 的秩被 M 唯一决定, 前面已经证明了. 我们又知道 $\text{Tor}(M)$ 是被 M 唯一决定, 因之下面的讨论可以限制在扭模的情形.

首先我们指出关于直和分解的一个简单事实. 设 M 为环 R 上的一个模, 有直和分解

$$M = \bigoplus_{k=1}^{m} M_k,$$

$a \in R$. 于是

$$aM = \bigoplus_{k=1}^{m} aM_k,$$

$$M/aM \cong \bigoplus_{k=1}^{m} M_k/aM_k,$$

即 aM 与 M/aM 有相应的直和分解.

为了讨论唯一性, 我们先证

引理 1 设 N 是主理想环 R 上一循环 p 模, p 是 R 中一素元素. 对于 R 中任一素元素 q, 我们有:

1) 当 q 与 p 不相伴, $qN = N$;

2) 当 q 与 p 相伴, N/qN 为循环 p 模, 且

$$\operatorname{ann}(N/qN) = (p).$$

证明 令 $N = Rb$, $\operatorname{ann}(b) = (p^i)$.

1) 如 q 与 p 不相伴, 则 $(p^i, q) = 1$. 有 $u, v \in R$ 使 $up^i + vq = 1$, 于是

$$b = vqb \in qN.$$

这就证明了 $N = qN$.

2) 当 q 与 p 相伴, 无妨设 $q = p$.

我们知道, 循环模的商模还是循环模, 而

$$\operatorname{ann}(N/pN) = (p)$$

是显然的. □

引理 2 设 M 是主理想环 R 上一有限生成的 p 模, p 为 R 中一素元素, $\operatorname{ann}(M) = (p)$, 则 M 的第一标准分解

$$M = M_1 \oplus \cdots \oplus M_r$$

中有 $\operatorname{ann}(M_i) = (p)$, $i = 1, \cdots, r$, 且 r 是唯一决定的.

证明 由 $M_i \subset M$ 可知 $\mathrm{ann}(M_i) \supset \mathrm{ann}(M)$. 在主理想环中素元素生成极大理想, 从而

$$\mathrm{ann}(M_i) = \mathrm{ann}(M) = (p), \quad i = 1, \cdots, r.$$

因为 $\mathrm{ann}(M) = (p)$, 所以 M 可以看作商环 $R/(p)$ 上的模. 我们知道, $R/(p)$ 是域, 因之 M 可以看作域 $R/(p)$ 上的一线性空间. r 正是这个线性空间的维数, 当然是唯一的. □

现在来证明唯一性. 设 M 是主理想环 R 上一有限生成的扭模, 它的第一标准分解是

$$M = \bigoplus_{i=1}^{s} \bigoplus_{j_i=1}^{r_i} N_{ij_i},$$
$$\mathrm{ann}(N_{ij_i}) = (p_i^{n_{ij_i}}), \quad i = 1, \cdots, s, \quad j_i = 1, \cdots, r_i.$$

令 q 为 R 中任一素元素. 我们有

$$M/qM \cong \bigoplus_{i=1}^{s} \bigoplus_{j_i=1}^{r_i} N_{ij_i}/qN_{ij_i}.$$

由引理 1, 当 q 不与 $p_1, \cdots, p_s$ 中任一个相伴时, 我们有

$$M/qM = \{0\}.$$

当 q 与 $p_1, \cdots, p_s$ 中某一个相伴, 譬如说 $q = p_1$, 则根据引理 1 与引理 2, 我们有

$$M/p_1M \cong N_{11}/p_1N_{11} \oplus \cdots \oplus N_{1r_1}/p_1N_{1r_1},$$

而 r_1 就是域 R/p_1R 上线性空间 M/p_1M 的维数. 换句话说, M/p_1M 在域 R/p_1R 上的维数就是元素组

$$\begin{array}{c} p_1^{n_{11}}, \cdots, p_1^{n_{1r_1}}, \\ \cdots\cdots\cdots\cdots \\ p_s^{n_{s1}}, \cdots, p_s^{n_{sr_s}} \end{array} \tag{5}$$

中 p_1 方幂的个数. 因之, r_1 与分解式无关, 是被 M 唯一决定的.

再看 p_1M/p_1^2M 在 R/p_1R 上的维数. 同样

$$p_1M/p_1^2M \cong p_1N_{11}/p_1^2N_{11} \oplus \cdots \oplus p_1N_{1r_1}/p_1^2N_{1r_1}.$$

显然

$$\mathrm{ann}(p_1N_{1j}) = (p_1^{n_{1j}-1}),$$

因之 p_1M/p_1^2M 在 R/p_1R 上的维数就是元素组

$$p_1^{n_{11}-1},\cdots,p_1^{n_{1r_1}-1}$$

中 p_1 的方幂的个数，或者说就是元素组

$$p_1^{n_{11}},\cdots,p_1^{n_{1r_1}}$$

中 p_1^t $(t\geq 2)$ 的个数.

一般地，$p_1^kM/p_1^{k+1}M$ 在 R/p_1R 上的维数就是元素组

$$p_1^{n_{11}},\cdots,p_1^{n_{1r_1}}$$

中 p_1^t $(t\geq k+1)$ 的个数.

由此可知，在域 R/p_1R 上，$p_1^{k-1}M/p_1^kM$ 的维数与 $p_1^kM/p_1^{k+1}M$ 的维数之差就是元素组

$$p_1^{n_{11}},\cdots,p_1^{n_{1r_1}}$$

中 p_1^k 出现的次数.

这就证明了

定理 11 设 M 为主理想环 R 上一有限生成的扭模，它的第一标准分解是

$$M=\bigoplus_{i=1}^{s}\bigoplus_{j_i=1}^{r_i}N_{ij_i},$$

$\operatorname{ann}(N_{ij_i})=(p_i^{n_{ij_i}})$. 元素组 (5) 在相伴的意义下是被 M 唯一决定的. □

由第一标准分解与第二标准分解的关系，同时也就证明了

定理 12 设 M 为主理想环 R 上一有限生成扭模，它的第二标准分解是

$$M=\bigoplus_{k=1}^{l}M_k,$$

$\operatorname{ann}(M_k)=(d_k)$, $d_k|d_{k-1}$, $k=2,\cdots,l$. 元素组

$$d_1,d_2,\cdots,d_l \tag{6}$$

在相伴的意义下是被 M 唯一决定的. □

定义 5 设 M 是主理想环 R 上一有限生成模. 由 $\operatorname{Tor}(M)$ 的第一标准分解所确定的元素组 (5) 称为 M 的 **初等因子**. 由 $\operatorname{Tor}(M)$ 的第二标准分解所确定的元素组 (6) 称为 M 的 **不变因子**.

由以上讨论可知，对于主理想环上的有限生成模 M，它的秩与初等因子或者秩与不变因子是刻画模 M 的结构的一组 **完全不变量**.

§5 第二标准分解的又一证明

在这一节我们要给出第二标准分解的另一个证明. 证明将利用主理想环上的矩阵. 证明的过程在一定的意义上是一个计算的过程, 因而也就给出了一个计算不变因子与秩的步骤.

设 M' 是主理想环 R 上一个有限生成模, $x_1,\cdots,x_m$ 为一组生成元, 作一个 m 秩自由 R- 模 $M, e_1,\cdots,e_m$ 为它的一组基, 于是映射

$$\eta: \sum_{i=1}^{m} a_i e_i \mapsto \sum_{i=1}^{m} a_i x_i, \quad a_i \in R$$

是 M 到 M' 的一个满同态, 记 $N = \ker(\eta)$, 则 $M/N \cong M'$. N 就是 M' 的生成元 x_i 的关系的总和. 反之, 任给 M 的一个子模 N, 可以作出一个有限生成 R-模 M'.

设 $f_1,\cdots,f_n$ 是 N 的一组生成元. 设

$$f_i = \sum_{j=1}^{m} a_{ji} e_j, \quad i = 1,\cdots,n.$$

写成

$$(f_1,\cdots,f_n) = (e_1,\cdots,e_m)A, \quad A = (a_{ij}), \tag{1}$$

这里 A 是一 $m\times n$ 矩阵. 作 M 的基变换, 设 $e'_1,\cdots,e'_m$ 为 M 的任一基. 令

$$(e_1,\cdots,e_m) = (e'_1,\cdots,e'_m)P,$$

$P = (p_{ij})$ 为 R 上一个 $m\times m$ 可逆矩阵. 反之, 若 P 为可逆, 则 $e'_1,\cdots,e'_m$ 为 M 的一基. 再利用 R 上一个 $n\times n$ 可逆矩阵 $Q = (q_{ij})$ 作 N 的生成元变换

$$(f_1,\cdots,f_n) = (f'_1,\cdots,f'_n)Q,$$

这里要求 Q 可逆, 为的是保证 $f'_1,\cdots,f'_n$ 仍是 N 的一组生成元, 于是

$$(f'_1,\cdots,f'_n) = (e'_1,\cdots,e'_m)PAQ^{-1}. \tag{2}$$

在给了 m 秩自由模 M 及它的一组基 $e_1,\cdots,e_m$, 矩阵 A 显然就刻画了 M 的子模 N, 从而也就刻画了商模 M/N. 以上的讨论说明了基与生成元的变换与矩阵的变换之间的关系. 为此我们给出

定义 6 设 A, B 为主理想环 R 上两个 $m\times n$ 矩阵. 若存在一个 $m\times m$ 可逆矩阵 $P = (p_{ij})$ 和一个 $n\times n$ 可逆矩阵 $Q = (q_{ij})$, $p_{ij}, q_{ij} \in R$, 使得

$$B = PAQ,$$

则 A, B 叫做在 R 上**等价**.

这个等价显然满足等价关系的三个条件.

下面我们来证明主理想环 R 上有限秩自由模的子模的不变量定理.

定理 13 设 M 为主理想环 R 上一个 m 秩自由模, N 为它的一个子模, 于是存在 M 的一基 $e_1, \cdots, e_m$ 使得 $d_1e_1, d_2e_2, \cdots, d_re_r$ 构成 N 的一基而且

$$d_i | d_{i+1}, \quad i = 1, \cdots, r-1,$$

$d_1, \cdots, d_r$ 除相差一个单位因子外由 N 唯一决定, $d_1, \cdots, d_r$ 叫做 N 的不变量, r 是子模 N 的秩, $m-r$ 是商模 M/N 的秩, $d_1, \cdots, d_r$ 是商模 M/N 的不变因子. □

根据上面的讨论, 与定理 13 等价的定理是

定理 14 设 A 为主理想环 R 上任一个 $m \times n$ 矩阵, 则 A 等价于下列矩阵 B

$$B = \begin{pmatrix} d_1 & & & & & & \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix},$$

其中 $d_1, \cdots, d_r$ 不为零, 且

$$d_i | d_{i+1}, \quad i = 1, \cdots, r-1.$$

$d_1, \cdots, d_r$ 除相差一个单位因子外由 A 唯一确定, $d_1, \cdots, d_r$ 叫做 A 的不变因子, B 叫做 A 的标准形.

在主理想环 R 内对每个非零元素 a 定义一个长度 $l(a)$. 如果 a 写成 s 个素元 $p_1, \cdots, p_s$ 的积, 则规定 $l(a) = s$. 如果 a 为单位, 规定 $l(a) = 0$. 如果 $a \sim b$, 则 $l(a) = l(b)$. 如果 a 为 b 的真因子, 则 $l(a) < l(b)$. 如果 $a | b$ 且 $l(a) = l(b)$, 则 $a \sim b$.

从线性代数我们知道, 矩阵的两行互换以及一行加上另一行的倍数可以由左乘一初等矩阵来实现, 同样, 列的相应变换可以由右乘一初等矩阵来实现. 因之, 定义 6 中矩阵的等价包含矩阵的上述行与列的变换.

为了证明定理 14, 先证

引理 设 A 为主理想环 R 上一 2×2 矩阵,

$$A=\begin{pmatrix} a & b \\ c & e \end{pmatrix}.$$

则 A 等价于矩阵

$$\begin{pmatrix} d & 0 \\ * & * \end{pmatrix},$$

其中 $d=(a,b),*,*$ 为 R 上适当的元素.

证明 由 $(a,b)=d$ 可知, 有 $u,v\in R$ 使

$$ua+vb=d,a=da_1,b=db_1,$$

两边消去 d, 即得

$$ua_1+vb_1=1.$$

作 2×2 矩阵

$$Q=\begin{pmatrix} u & -b_1 \\ v & a_1 \end{pmatrix}.$$

显然 $|Q|=1,Q$ 可逆.

$$\begin{pmatrix} a & b \\ c & e \end{pmatrix}\begin{pmatrix} u & -b_1 \\ v & a_1 \end{pmatrix}=\begin{pmatrix} d & 0 \\ * & * \end{pmatrix}. \quad \square$$

同样可证, 矩阵 A 等价于

$$\begin{pmatrix} d & * \\ 0 & * \end{pmatrix},$$

其中 $d=(a,c)$.

定理 14 的证明: 设 $A=(a_{ij})$ 为主理想环 R 上一 $m\times n$ 矩阵.

如 $A=0$, 则结论显然. 下面设 $A\neq 0$. 经过行列互换, 无妨假定元素 $a_{11}\neq 0$ 且长度最小.

如 $a_{11}|a_{1j}, j=2,\cdots,n$, 则第 j 列减去第一列的适当倍数, $j=2,\cdots,n$ 可得一矩阵, 它的第一行中除去 $a_{11}\neq 0$ 外, 其余全为 0. 如果有 j_0 使 $a_{11}\nmid a_{1j_0}$, 经过列的互换, 无妨设 $a_{11}\nmid a_{12}$, 则由引理, 有 2×2 矩阵 Q_1 使

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}Q_1=\begin{pmatrix} d & 0 \\ * & * \end{pmatrix},$$

其中 $d=(a_{11},a_{12})$. 令

$$Q=\begin{pmatrix} Q_1 & 0 \\ 0 & E \end{pmatrix}.$$

其中 E 为 $(n-2)\times(n-2)$ 单位矩阵. 于是在矩阵

$$AQ$$

中第一行第一列的元素为 d. 由 $l(a_{11})$ 最小与 $a_{11}\nmid a_{12}$ 可知 $l(d)<l(a_{11})$. 这就是说, 只要第一行的元素中有一个不能被 a_{11} 整除, 我们就得到一个与之等价的矩阵, 它的 a_{11} 有更小的长度. 由于非零元素的长度为非负整数, 因之反复应用引理, 我们总可以得到一个与 A 等价的矩阵, 它的第一行为

$$a_{11},0,\cdots,0.$$

对第一列作同样的讨论, 可知 A 一定等价于一矩阵

$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix}.$$

如果在矩阵 B 中有一个元素不被 a_{11} 整除, 那么把这个元素所在的行加到第一行, 又回到前面讨论的情形, 这样, 可以再一次降低第一行第一列元素的长度. 反复若干次之后, 我们得到一个与 A 等价的矩阵

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A_1 & \\ 0 & & & \end{pmatrix},$$

其中 $d_1\neq 0$, 且 d_1 整除 A_1 中每个元素. 对 A_1 作同样的变换, 我们又得到一等价的矩阵

$$\begin{pmatrix} d_1 & 0 & \\ 0 & d_2 & \\ & & A_2 \end{pmatrix},$$

其中 $d_1\neq 0, d_2\neq 0, d_1|d_2$, d_2 整除 A_2 中每个元素. 这里 $d_1|d_2$ 是由于 d_2 总是 A_1 中元素的组合.

这样下去，我们就证明了 A 等价于一矩阵

$$\begin{pmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix},$$

其中 $d_i \neq 0$, $i = 1, \cdots, r$, $d_i | d_{i+1}$, $i = 1, \cdots, r-1$.

至于唯一性可由上一节所证的唯一性推出，这里就不另证了. □

当 $R = \mathbf{Z}$ 或 $F[\lambda]$, F 为一域时，定理 14 的证明实际上给出了一个算法. 由这个算法可以算出有限生成模的秩与不变因子.

由定理中的唯一性，即得

推论 *设 A, B 为主理想环 R 上两个 $m \times n$ 矩阵. 则 A, B 等价的充分必要条件是它们有相同的标准形或者有相同的不变因子.* □

§6 应用

我们应用以上的结论来讨论两种重要的情况，即整数环 $\mathbf{Z}$ 上的有限生成模和一元多项式环 $F[\lambda]$ 上有限生成模的构造，其中 F 为一域.

1. 有限生成阿贝尔群

设 G 为一个有限生成阿贝尔群，即 G 为一个有限生成 $\mathbf{Z}$- 模，根据定理 4,G 可以写成一个扭子模 G_0 和一个自由子模 G_1 的直和， G_1 的秩是 G 的一个不变量. 设 G_1 的秩为 r, 则 $G_1 \cong \mathbf{Z}^{(r)}$.

扭子模 G_0 也是有限生成的，设 $x_1, \cdots, x_m$ 为它的一组生成元， x_i 的阶为 n_i. 于是 G_0 的每个元素 x 可以表成 $x = x_1^{r_1} \cdots x_m^{r_m}$, $0 \leq r_i \leq n_i - 1$. 因此，一个有限生成的扭 $\mathbf{Z}$- 模是一个有限阿贝尔群.

根据定理 6, 一个有限阿贝尔群 G_0 可以分解成它的 p 分量 $G_{p_1}, \cdots, G_{p_t}$ 的直和，每个 G_{p_i} 就是 G_0 的西罗 p_i- 子群，有限阿贝尔群的西罗 p- 子群是唯一的.

根据定理 7, 有限交换 p- 群 G_p, p 为一个素数，可以分解成一些循环 p- 子群的直和. 设在直和分解中出现的 p- 子群的阶记为 $p^{e_1}, p^{e_2}, \cdots$, 而且 $e_1 \geq e_2 \geq \cdots$, 则 $p^{e_1}, p^{e_2}, \cdots$ 是 G_p 的一组不变量.

这样秩 r 和阶 $p_i^{e_{ij}}$, $i = 1, 2, \cdots, t, j = 1, 2, \cdots$, 就构成有限生成阿贝尔群 G 的一组完全不变量. 总结以上讨论得

定理 15 一个有限生成的阿贝尔群 G 可以分解成 r 个无限循环子群与若干个有限循环 p- 子群的直和. r 和有限循环 p- 子群的阶 $p_i^{e_{ij}}$, $i=1,2,\cdots,t, j=1,2,\cdots$, 构成 G 的一组完全不变量, 即两个有限生成阿贝尔群同构的充要条件是它们的不变量相同. □

例 一个 24 阶阿贝尔群互不同构的类型只有三种, 用不变量写出就是 3,8; 3,4,2 和 3,2,2,2 三种. 即一种是一个 3 阶子群和一个 8 阶循环子群的直和; 一种是一个 3 阶子群, 一个 4 阶循环子群和一个 2 阶子群的直和; 一种是一个 3 阶子群, 和 3 个 2 阶子群的直和. 容易证明这三种类型的阿贝尔群都存在.

2. 有限维线性空间的单个线性变换

设 F 为一域, V 为 F 上 n 维线性空间, $\boldsymbol{A}$ 为 V 的一个线性变换. 设 $u_1,\cdots,u_n$ 为 V 的一 F- 基, $\boldsymbol{A}$ 在基 $u_1,\cdots,u_n$ 下的矩阵为 A, 则

$$\boldsymbol{A}(u_1,\cdots,u_n)=(u_1,\cdots,u_n)A.$$

设 $v_1,\cdots,v_n$ 为 V 的另一基, 并设 $(v_1,\cdots,v_n)=(u_1,\cdots,u_n)P$, 则 $\boldsymbol{A}$ 在基 $v_1,\cdots,v_n$ 下的矩阵 $B=P^{-1}AP$. 我们的问题是求一适当的基 $v_1,\cdots,v_n$ 使得 $\boldsymbol{A}$ 在 $v_1,\cdots,v_n$ 下的矩阵具有标准的形状.

为了解决上面的问题, 将 V 看作 $F[\lambda]$- 模:

$$f(\lambda)\cdot x=f(\boldsymbol{A})\cdot x,\ x\in V, f(\lambda)\in F[\lambda].$$

若 V 分解成两个 $F[\lambda]$- 子模 V_1,V_2 的直和, 则 V_1,V_2 就是 $\boldsymbol{A}$ 的不变子空间. 分别在 V_1,V_2 内取基使得它们构成 V 的一基, 在这基下 $\boldsymbol{A}$ 的矩阵等于两个级数较小的矩阵的准对角形. 由此可见, 求 $\boldsymbol{A}$ 的矩阵的标准形状的问题和 V 作为 $F[\lambda]$- 模的分解有密切的关系.

首先 V 是一个有限生成 $F[\lambda]$- 模. 因为 F- 基 $u_1,\cdots,u_n$ 就是一组生成元, 而且根据线性代数的结果, V 是一个扭模. 对于每个元素 $x\in V$, $\mathrm{ann}(x)=(m(\lambda))$, $m(\lambda)$ 是 x 的 **极小多项式**. 若 $x\neq 0$, 则 $\deg m(\lambda)>0$.

按照定理 12, V 可以分解成一些循环子模的直和

$$V=F[\lambda]\cdot z_1\oplus\cdots\oplus F[\lambda]\cdot z_s,$$

使得 $\mathrm{ann} z_i=(d_i(\lambda))$, $(d_1(\lambda))\supset(d_2(\lambda))\supset\cdots\supset(d_s(\lambda))$, $d_1(\lambda),\cdots,d_s(\lambda)$ 不为零. $d_1(\lambda),\cdots,d_s(\lambda)$ 叫做线性变换 $\boldsymbol{A}$ 的不变因子.

1) 有理标准形

每个循环子模 $V_i=F[\lambda]\cdot z_i$ 作为 F- 模都是 $\boldsymbol{A}$ 的不变线性子空间, 它的维数 $=\deg d_i(\lambda)=n_i$, 而且 $z_i,\lambda z_i,\cdots,\lambda^{n_i-1}z_i$ 是 V_i 的一基. 设 $d_i(\lambda)=\lambda^{n_i}+$

$b_{in_i-1}\lambda^{n_i-1}+\cdots+b_{i0}$, 则 $\boldsymbol{A}$ 在 V_i 内诱导出的线性变换 $\boldsymbol{A}_i$ 在基 $z_i,\lambda z_i,\cdots,\lambda^{n_i-1}z_i$ 下的矩阵为

$$B_i=\begin{pmatrix} 0 & 0 & \cdots & 0 & -b_{i0} \\ 1 & 0 & \cdots & 0 & -b_{i1} \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 & -b_{in_i-2} \\ 0 & \cdots & 0 & 1 & -b_{in_i-1} \end{pmatrix},$$

B_i 叫做多项式 $d_i(\lambda)$ 的 **相伴矩阵**.

证明 已经知道对于 $x\in V_i$, $\lambda\cdot x\in V_i$, 因而 V_i 是 $\boldsymbol{A}$ 的不变子空间. 再确定 V_i 的维数. 我们知道对任何 $f(\lambda)\in F[\lambda]$, $f(\lambda)\cdot z_i=0$ 的充分必要条件是 $d_i(\lambda)|f(\lambda)$. 由此可知 $z_i,\lambda z_i,\cdots,\lambda^{n_i-1}z_i$ 在 F 上线性无关. 对于任意 $x\in V_i$, x 可表成 $x=f(\lambda)\cdot z_i$, 应用除法算式 $f(\lambda)=q(\lambda)\cdot d_i(\lambda)+r(\lambda)$, $\deg r(\lambda)<\deg d_i(\lambda)$. 于是 $x=f(\lambda)\cdot z_i=q(\lambda)\cdot d_i(\lambda)\cdot z_i+r(\lambda)\cdot z_i=r(\lambda)\cdot z_i$ 是 $z_i,\lambda z_i,\cdots,\lambda^{n_i-1}z_i$ 的线性组合, 所以 $\dim V_i=n_i$ 而且 $z_i,\cdots,\lambda^{n_i-1}z_i$ 是 V_i 的一基. 由计算

$$\begin{aligned}
&\boldsymbol{A}_i\cdot z_i=\lambda z_i,\\
&\boldsymbol{A}_i\cdot\lambda z_i=\lambda^2 z_i,\\
&\cdots\cdots\\
&\boldsymbol{A}_i\cdot\lambda^{n_i-2}z_i=\lambda^{n_i-1}z_i,\\
&\boldsymbol{A}_i\cdot\lambda^{n_i-1}z_i=-b_{i0}z_i-b_{i1}\lambda z_i-\cdots-b_{in_i-1}\lambda^{n_i-1}z_i,
\end{aligned}$$

所以 A_i 在基 $z_i,\lambda z_i,\cdots,\lambda^{n_i-1}z_i$ 下的矩阵为 B_i. □

由于 V 是 $V_1,\cdots,V_s$ 的直和, $z_1,\cdots,\lambda^{n_1-1}z_1,\cdots,z_s,\cdots,\lambda^{n_s-1}z_s$ 构成 V 的一基, 在这组基下 $\boldsymbol{A}$ 的矩阵为

$$B=\begin{pmatrix} B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_s \end{pmatrix},$$

其中每个 B_i 是 $d_i(\lambda)$ 的相伴矩阵. B 叫做线性变换 $\boldsymbol{A}$ 的 **有理标准形**.

从 $F[\lambda]$- 模 V 的分解以及 $\boldsymbol{A}$ 的不变因子得到几个事实:

i) $\sum\deg d_i(\lambda)=\dim V$.

这是因为 $\dim V=\sum\dim V_i=\sum\deg d_i(\lambda)$.

ii) V 的零化子 $=(d_s(\lambda))$, 即 $d_s(\lambda)$ 是线性变换 $\boldsymbol{A}$ 的极小多项式.

这是因为，对任意 $f(\lambda)\in \text{ann}(V)$，有 $f(\lambda)\cdot z_s=0$，从而 $d_s(\lambda)|f(\lambda)$，$f(\lambda)\in (d_s(\lambda))$，$\text{ann}(V)\subset (d_s(\lambda))$；反之，设 $f(\lambda)\in (d_s(\lambda))$. 于是 $d_i(\lambda)|d_s(\lambda)|f(\lambda)$，从而 $f(\lambda)\cdot z_i=0$（对所有 i），所以 $f(\lambda)\cdot x=0$（对所有 $x\in V$），于是 $f(\lambda)\in \text{ann}V$. $(d_s(\lambda))\subset \text{ann}(V)$，因之 $\text{ann}(V)=(d_s(\lambda))$.

多项式 $f(\lambda)=|\lambda E-A|$ 叫做线性变换 $\boldsymbol{A}$ 的**特征多项式**. 它与 V 的 F- 基的选取无关. 因为若从基 u_i 转换成基 v_i，$\boldsymbol{A}$ 的矩阵从 A 转换成 $B=P^{-1}AP$，于是

$$\begin{aligned}|\lambda E-B|&=|\lambda E-P^{-1}AP|=|P^{-1}(\lambda E-A)P|\\&=|P^{-1}||\lambda E-A||P|=|\lambda E-A|\\&=f(\lambda).\end{aligned}$$

iii) $\boldsymbol{A}$ 的特征多项式 $|\lambda E-A|=\prod_{i=1}^{s}d_i(\lambda)$，因此 $\boldsymbol{A}$ 的特征多项式和它的极小多项式有相同的不可约因子.

这是因为，只要取 A 的线性变换 $\boldsymbol{A}$ 的有理标准形 B，于是

$$|\lambda E-A|=|\lambda E-B|=\prod_{i=1}^{s}|\lambda E_{n_i}-B_i|.$$

计算

$$|\lambda E_{n_i}-B_i|=\begin{vmatrix}\lambda & 0 & \cdots & 0 & b_{i0}\\ -1 & \lambda & \ddots & \vdots & b_{i1}\\ 0 & -1 & \ddots & 0 & \vdots\\ \vdots & & \ddots & \lambda & b_{in_i-2}\\ 0 & \cdots & 0 & -1 & \lambda+b_{in_i-1}\end{vmatrix}.$$

将第 n_i 行的 λ 倍加到第 n_i-1 行，然后将新得到的行列式的第 n_i-1 行的 λ 倍加到第 n_i-2 行，如此进行下去，将最后得到的行列式按第一行展开，即得

$$|\lambda E_{n_i}-B_i|=d_i(\lambda).$$

由 ii) 和 iii) 得到

iv) $\boldsymbol{A}$ 是 $\boldsymbol{A}$ 的特征多项式 $f(\lambda)$ 的根.

最后一个事实也可以直接证明之.

2) 若尔当标准形

假设 $F[\lambda]$- 模 V 的不变因子 $d_i(\lambda)$ 在 $F[\lambda]$ 内部可以分解成一次因式的方幂的积，则线性变换 $\boldsymbol{A}$ 的矩阵还有第二种标准形，即**若尔当标准形**. 当 F 为复数

域时，这个假设对任何线性变换都是成立的．设 $d_s(\lambda)$ 在 $F[\lambda]$ 内分解成

$$d_s(\lambda)=\prod_{i=1}^{r}(\lambda-\lambda_j)^{e_{s_j}},\quad e_{s_j}\geq 1,\ \lambda_i\neq\lambda_j, i\neq j.$$

于是 $d_1(\lambda),\cdots,d_{s-1}(\lambda)$ 都可分解成

$$d_i(\lambda)=\prod_{j=1}^{r}(\lambda-\lambda_j)^{e_{i_j}},\quad e_{i_j}\geq 0.$$

由于 $d_i(\lambda)|d_{i+1}(\lambda)$，有

$$0<e_{1_j}\leq e_{2_j}<\cdots\leq e_{s_j},\quad j=1,\cdots,r.$$

根据定理 6,$F[\lambda]\cdot z_i$ 可以分解成一些循环 $(\lambda-\lambda_j)$- 模的直和

$$F[\lambda]\cdot z_i=\bigoplus_j F[\lambda]\cdot z_{i_j},$$

其中 $\mathrm{ann}(z_{i_j})=(\lambda-\lambda_j)^{e_{i_j}}$，$e_{i_j}\geq 1$．于是

$$V=\bigoplus_i\bigoplus_j F[\lambda]\cdot z_{i_j}.$$

每个 $F[\lambda]\cdot z_{i_j}$ 是 $\boldsymbol{A}$ 的一个循环不变子空间，由 $\boldsymbol{A}$ 在其中诱导出的线性变换只有一个特征值 λ_j，而且它只有一个初等因子 $(\lambda-\lambda_j)^{e_{i_j}}$．这个初等因子也是它的极小多项式．

设 $F[\lambda]\cdot z$ 是上述 V 的分解式中的任一项，$\mathrm{ann}(z)=(\lambda-\lambda_1)^e$，$e\geq 1$，$(\lambda-\lambda_1)^e$ 是它的唯一的一个不变因子，$F[\lambda]\cdot z$ 简记作 V_1，仿上可知 $z,\lambda z,\cdots,\lambda^{e-1}z$ 是 V_1 的一 F- 基，由此可知，$z,(\lambda-\lambda_1)z,\cdots,(\lambda-\lambda_1)^{e-1}z$ 也是 V_1 的一 F- 基，$\boldsymbol{A}$ 在 V_1 内诱导出的线性变换 $\boldsymbol{A}_1$ 在基 $z,(\lambda-\lambda_1)z,\cdots,(\lambda-\lambda_1)^{e-1}\cdot z$ 下的矩阵由计算

$$\begin{aligned}
&\boldsymbol{A}\cdot z=\lambda z=\lambda_1 z+(\lambda-\lambda_1)z,\\
&\boldsymbol{A}(\lambda-\lambda_1)z=\lambda(\lambda-\lambda_1)z=\lambda_1(\lambda-\lambda_1)z+(\lambda-\lambda_1)^2 z,\\
&\cdots\cdots\\
&\boldsymbol{A}(\lambda-\lambda_1)^{e-2}z=\lambda_1(\lambda-\lambda_1)^{e-2}z+(\lambda-\lambda_1)^{e-1}z,\\
&\boldsymbol{A}(\lambda-\lambda_1)^{e-1}z=\lambda_1(\lambda-\lambda_1)^{e-1}z
\end{aligned}$$

(因为 $(\lambda-\lambda_1)^e z=0$) 可知是

$$C=\begin{pmatrix} \lambda_1 & & & & \\ 1 & \lambda_1 & & & \\ & 1 & \ddots & & \\ & & & \ddots & \\ & & & 1 & \lambda_1 \end{pmatrix}.$$

矩阵 C 叫做 e 级 **若尔当块**, 属于特征值 λ_1.

于是在每个循环 $(\lambda-\lambda_j)$- 模 $F[\lambda]\cdot z_{i_j}$ 中取如上的标准基 $z_{i_j},(\lambda-\lambda_j)z_{i_j},\cdots,(\lambda-\lambda_j)^{e_{i_j}-1}\cdot z_{i_j}$, 把这些标准基按顺序连接起来就构成 V 的一标准基, 在这标准基下 A 的矩阵就是若干个若尔当块的准对角形:

$$D=\begin{pmatrix} C_1 & & & \\ & C_2 & & \\ & & \ddots & \\ & & & C_t \end{pmatrix},$$

其中每个 C_i 是属于 A 的特征值的若尔当块, 这些若尔当块和 A 的初等因子 $(\lambda-\lambda_j)^{e_{ij}}$ 成一一对应. 矩阵 D 叫做 **若尔当标准形**.

3. 线性变换的不变因子的计算

设 V 为域 F 上一个 n 维线性空间, $\boldsymbol{A}$ 为 V 的一个线性变换, V 看作一个 $F[\lambda]$- 模: $\lambda\cdot x=\boldsymbol{A}(x)$, $x\in V$. 设 $u_1,\cdots,u_n$ 为 V 的一 F- 基, $\boldsymbol{A}$ 在基 $u_1,\cdots,u_n$ 下的矩阵 $A=(a_{ij})$:

$$\boldsymbol{A}(u_i)=\lambda u_i=\sum_{j=1}^{n}a_{ji}u_j,\ \ i=1,2,\cdots,n.$$

为了计算 $\boldsymbol{A}$ 的不变因子, 作一个 n 秩自由 $F[\lambda]$- 模 M, $e_1,\cdots,e_n$ 为它的一基, 作 M 到 V 的 $F[\lambda]$- 同态

$$\eta:\sum_{i=1}^{n}g_i(\lambda)e_i\mapsto\sum_{i=1}^{n}g_i(\lambda)u_i.$$

令 $N=\ker(\eta)$, 由上式可知

$$\begin{cases} (\lambda-a_{11})u_1-a_{21}u_2-\cdots-a_{n1}u_n=0, \\ -a_{12}u_1+(\lambda-a_{22})u_2-\cdots-a_{n2}u_n=0, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ -a_{1n}u_1-a_{2n}u_2-\cdots+(\lambda-a_{nn})u_n=0. \end{cases}$$

设

$$\begin{cases} f_1 = (\lambda - a_{11})e_1 - a_{21}e_2 - \cdots - a_{n1}e_n, \\ f_2 = -a_{12}e_1 + (\lambda - a_{22})e_2 - \cdots - a_{n2}e_n, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ f_n = -a_{1n}e_1 - a_{2n}e_2 - \cdots + (\lambda - a_{nn})e_n. \end{cases}$$

显然 $f_i \in N\ (i = 1, 2, \cdots, n)$. 我们来证明，元素 $f_1, \cdots, f_n$ 构成 N 的一基.

将 N 的元素改写成如下的形式

$$h = \lambda^m \sum_i b_{mi}e_i + \lambda^{m-1} \sum_i b_{m-1i}e_i + \cdots + \sum_i b_{0i}e_i,$$

其中 $b_{ij} \in F$. 每个 f_i 也可写成

$$f_i = \lambda e_i - \sum_j a_{ji}e_j.$$

首先证明 f_i 是 N 的一组生成元. 设 $h \in N$, 对 h 的 "次数"m 作归纳法. 当 $m = 0$ 时, $\eta(h) = \sum_i b_{0i}u_i = 0$, 从而 $b_{0i} = 0$, $i = 1, \cdots, n, h = 0$, 0 当然可表成 f_i 的组合. 假设当 h 的 "次数"$< m$, $m > 0$ 时, h 可表成 f_i 的组合, 求证当 h 的 "次数"$= m$ 时, 也如此. 为此, 在 h 的表达式中将头一个和号中的 λe_i 换成 $f_i + \sum_j a_{ji}e_i$, 得

$$\begin{aligned} h &= \lambda^{m-1} \sum_i b_{mi}f_i + \lambda^{m-1} \sum_i \sum_j b_{mi}a_{ji}e_i \\ &\quad + \lambda^{m-1} \sum_i b_{m-1i}e_i + \cdots + \sum_i b_{0i}e_i, \end{aligned}$$

或者

$$h = \lambda^{m-1} \sum_i b_{mi}f_i + h_1,$$

$\eta(h) = \eta(h_1) = 0, h_1 \in N$ 而且 h_1 的 "次数"$< m$. 根据归纳法假设 h_1 可表成 f_i 的组合, 因而 h 也表成了 f_i 的组合, 所以 f_i 是 N 的一组生成元.

其次证明 $f_1, \cdots, f_n$ 在 $F[\lambda]$ 上线性无关. 反证法, 假设 f_i 在 $F[\lambda]$ 上线性相关, 于是存在一组不全为零的多项式 $g_i(\lambda) \in F[\lambda]$ 使得

$$\sum_i g_i(\lambda)f_i = 0.$$

在非零的 $g_i(\lambda)$ 中有一个次数最高的. 为方便起见, 不妨设 $g_1(\lambda) \neq 0$ 且 $\deg g_1(\lambda) \geq \deg g_i(\lambda)$, $i \geq 2$. 将上式左端整理成 $e_1, \cdots, e_n$ 的组合, e_1 的系数为

$$q(\lambda) = \lambda g_1(\lambda) - a_{11}g_1(\lambda) - a_{12}g_2(\lambda) - \cdots - a_{1n}g_n(\lambda).$$

而 $\deg \lambda g_1(\lambda) = 1 + \deg g_1(\lambda) > \deg a_{1i}g_i(\lambda)$, $i = 1, \cdots, n$, $q(\lambda) = 0$, 这引出矛盾，所以 $f_1, \cdots, f_n$ 在 $F[\lambda]$ 上线性无关， $f_1, \cdots, f_n$ 构成 N 的一基.

因而我们有

$$(f_1, \cdots, f_n) = (e_1, \cdots, e_n)(\lambda E - A).$$

$\lambda E - A$ 叫做矩阵 A 的 **特征矩阵**, 根据上面的讨论我们得到

定理 16 *设 V 为域 F 上一 n 维线性空间， $\boldsymbol{A}$ 为 V 的一个线性变换， A 为 $\boldsymbol{A}$ 在 V 的任一基下的矩阵，设 $d_1, \cdots, d_n$ 为 A 的特征矩阵 $\lambda E - A$ 的不变因子，而且 $d_1 = \cdots = d_t = 1 \neq d_{t+1}$, 则 $d_{t+1}, \cdots, d_n$ 就是 A 的全部不变因子.* □

这个定理给我们计算线性变换的不变因子的一个方法.

例 设 V 为有理数域 $\mathbf{Q}$ 上 3 维线性空间， $\boldsymbol{A}$ 为 V 的一个线性变换，在 V 的基 u_1, u_2, u_3 下的矩阵为

$$A = \begin{pmatrix} -3 & -1 & -1 \\ -2 & -2 & -1 \\ 6 & 3 & 2 \end{pmatrix},$$

求 A 的不变因子和 $\boldsymbol{A}$ 的两种标准形.

首先应用初等变换求特征矩阵的标准形

$$\lambda E - A = \begin{pmatrix} \lambda+3 & 1 & 1 \\ 2 & \lambda+2 & 1 \\ -6 & -3 & \lambda-2 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & \lambda+3 \\ 1 & \lambda+2 & 2 \\ \lambda-2 & -3 & -6 \end{pmatrix}$$

$$\to \begin{pmatrix} 1 & 1 & \lambda+3 \\ 0 & \lambda+1 & -\lambda-1 \\ 0 & -(\lambda+1) & -\lambda^2-\lambda \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda+1 & -(\lambda+1) \\ 0 & -(\lambda+1) & -\lambda(\lambda+1) \end{pmatrix}$$

$$\to \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda+1 & 0 \\ 0 & -(\lambda+1) & -(\lambda+1)^2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda+1 & 0 \\ 0 & 0 & -(\lambda+1)^2 \end{pmatrix}$$

$$\to \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda+1 & 0 \\ 0 & 0 & (\lambda+1)^2 \end{pmatrix},$$

所以 A 的不变因子为 $\lambda+1, (\lambda+1)^2$, 与它们相对应的有理块分别为

$$(-1) \text{ 和 } \begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix},$$

所以 A 的有理标准形为

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & -2 \end{pmatrix}.$$

与 $\lambda+1$ 和 $(\lambda+1)^2$ 对应的若尔当块分别为

$$(-1) \text{ 和 } \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix},$$

所以 A 的若尔当标准形为

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}.$$

习 题

1. 设 M 为主理想环 R 上的有限生成模, $x_1,\cdots,x_n$ 是一组生成元, $y_1 = a_1x_1 + \cdots + a_nx_n$. 如果 $(a_1,\cdots,a_n)=1$, 则存在 $y_2,\cdots,y_n$, 使 $y_1,y_2,\cdots,y_n$ 是 M 的一组生成元.

2. 设 M 为主理想环 R 上一 n 秩的自由模, $x_1,\cdots,x_n$ 是一组基, $y_1=a_1x_1+\cdots+a_nx_n, y_2=b_1x_1+\cdots+b_nx_n$. 如果 $(a_1,\cdots,a_n)\sim(b_1,\cdots,b_n)$, 则存在 M 的一个模自同构 η 使 $\eta(y_1)=y_2$.

3. 证明, 主理想环 R 上一扭模是不可约的 (即没有非平凡的子模) 充分必要条件为 $M=Rz$, 且 $\mathrm{ann}(z)=(p)$, 这里 p 是一个素元素.

4. 设 M 为主理想环 R 上一有限生成的扭模. 证明, M 不能分解成两个非零子模的直和的充分必要条件为 $M=Rz$, 且 $\mathrm{ann}(z)=(p^e)$, 这里 p 是 R 的一个素元素, $e\geq 1$.

5. 设 M 是主理想环 R 上的模. M 的一个子模 N 叫做**纯子模**, 如果方程 $ax=z$, $a\in R, z\in N$, 在 M 中有解, 则在 N 中也有解. 证明, 如果子模 N 是 M 的一个直和项, 则 N 是一纯子模.

6. 设 M 是主理想环 R 上的模. 如果 N 是一个纯子模, 则在每个陪集 $x+N$ 中有一元素 y 使 $\mathrm{ann}(y)=\mathrm{ann}(\bar{x})$, 这里 $\bar{x}$ 表示 x 在商模 M/N 中的象.

7. 设 M 为主理想环 R 上一有限生成模. 如果 M 的一个子模是纯的, 则 N 是 M 的一个直和项.

8. 设 M 为主理想环 R 上一有限生成扭模, $z\in M$ 适合条件 $\mathrm{ann}(z)\subset\mathrm{ann}(x)$ 对所有的 $x\in M$, 则 Rz 为一纯子模, 因而 Rz 是 M 的一个直和项.

9. 设 R 为一欧几里得整环, $A\in M_n(R)$. 证明: 如果 $|A|=1$, 则 A 可以表成一些初等矩阵的乘积.

10. 设 R 为一主理想环, $A \in M_n(R)$. 证明存在一可逆矩阵 $Q \in M_n(R)$, 使 AQ 为下三角形.

11. 设 R 为一主理想环. 证明 $M_n(R)$ 的每个左理想都是主理想.

12. 设 R 为一交换环. 如果 R 上的自由模的子模都是自由的, 则 R 为一主理想环.

13. 设 R 为一主理想环. R 上线性方程组

$$\begin{aligned} a_{11}x_1+\cdots+a_{1n}x_n&=b_1,\\ &\cdots\cdots\\ a_{s1}x_1+\cdots+a_{sn}x_n&=b_s, \end{aligned}$$

其中 $a_{ij}, b_k \in R$, 在 R 中有解的充分必要条件是 $A=(a_{ij})$ 的所有 l 级子式的最大公因式和增广矩阵的所有 l 级子式的最大公因子相同, $l=1,2,\cdots$.

14. 设 R 为主理想环, $A, B \in M_n(R)$, $|AB| \neq 0$, 对角形矩阵 $[a_1, a_2, \cdots, a_n]$, $[b_1, b_2, \cdots, b_n]$ 与 $[c_1, c_2, \cdots, c_n]$ 分别是 A, B 与 AB 的标准形. 证明

$$a_i|c_i, \quad b_i|c_i, \quad i=1,\cdots,n.$$

15. 试定出全部阶为 392 的交换群互不同构的类型.

16. 算出 $(3,3^2,3^2,3^5,3^7)$ 类型的交换群中 9 阶子群的个数.

17. 证明, 恰有四个有限生成交换群, 它们只要两个自同构.

18. 算出下列矩阵的初等因子, 不变因子, 有理标准形, 若尔当标准形:

$$\text{(i)} \begin{pmatrix} 1 & 0 & -2 \\ 2 & 6 & 8 \\ -1 & -3 & -4 \end{pmatrix}, \qquad \text{(ii)} \begin{pmatrix} 4 & -2 & -1 \\ 5 & -2 & -1 \\ -2 & 1 & 1 \end{pmatrix},$$

$$\text{(iii)} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 4 & 3 & -2 & 0 \\ -2 & 1 & 5 & 0 \\ 2 & 0 & -1 & 3 \end{pmatrix}, \qquad \text{(iv)} \begin{pmatrix} 3 & 2 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -2 & -2 & -2 & 1 \\ -2 & 0 & -3 & 2 \end{pmatrix}.$$

19. 设交换群 G 由 a_1, a_2, a_3, a_4 生成, 它们之间有联系

$$\begin{aligned} 2a_1 - a_2 + 5a_3 &= 0,\\ a_2 - 3a_3 &= 0,\\ 3a_1 \qquad - 7a_3 &= 0. \end{aligned}$$

求 G 的不变量.

20. 设 A 为 n 维线性空间 V 的一线性变换. 证明: V 为一循环空间的充分必要条件是 A 的特征多项式与极小多项式相等.

21. 设 F 为一个特征为 0 的域, $A \in M_n(F)$. 证明: A 为幂零的充分必要条件是 $\mathrm{tr}(A^i)=0$, $i=1,2,\cdots,n$, 其中 $\mathrm{tr}(X)$ 表示矩阵 X 主对角线上元素的和.

22. 设 $A \in M_n(\mathbf{C})$. 证明： A 相似于一对角矩阵的充分必要条件是 A 的极小多项式只有单根.

23. 设 $A \in M_n(F), F$ 为一域. 证明 A 与 A^T 相似.

24. 设 $A, B \in M_n(\mathbf{C})$. 证明： A, B 相似的充分必要条件是对任意复数 α 有

$$秩(\alpha E - A)^k = 秩(\alpha E - B)^k, \quad k = 1, \cdots, n.$$

25. 令 $\mathbf{F}_p$ 为 p 个元素的素域. 在 $M_n(\mathbf{F}_p)$ 中, 证明

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

与

$$B = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

相似.

26. 设 F 为一域, 证明：矩阵 $A, B \in M_n(F)$ 相似的充分必要条件是特征矩阵 $\lambda E - A$ 与 $\lambda E - B$ 等价.

第七章　域的基本概念

简单说来，域是具有双重群结构的代数系统，它既是一个加法群，又是一个乘法交换群 (0 除外)，而且加法和乘法由分配律联系起来．域的几个典型例子有有理数域、实数域、复数域、代数函数域等． 19 世纪 30 年代伽罗瓦发现了有限域． 20 世纪初亨泽尔 (Hensel) 发现了 p- 进数域．它们丰富了域的内容．不久斯泰尼茨 (Steinitz) 发表了他对抽象域所作的综合研究．本章所要介绍的就是其中的几个基本概念，代数扩张重点在有限扩张、正规扩张和可分扩张等．域扩张这个概念是研究域的一般方法．

§1　单扩张

域的特征是刻画域的一个基本的量．第一章告诉我们，任何一个域 K 的单位元素 e 通过加法生成一个子环 $P=\{n\cdot e\,|\,n\in\mathbf{Z}\}$．当 K 的特征 $\chi(K)=0$ 时，$P\cong\mathbf{Z}$，因而 P 的商域与有理数域 $\mathbf{Q}$ 同构．将 $n\cdot e$ 与 n 等同，则 $\mathbf{Q}$ 可看作 K 的子域，是由单位元素 e 生成的子域；当 $\chi(K)=p$ 素数时， $P\cong\mathbf{F}_p\cong\mathbf{Z}/(p)$．$P$ 已是 p 个元素的子域．同样 $\mathbf{F}_p$ 可看作 K 的子域，仍是由单位元素 e 生成的子域．这种子域具有如下的特点：

1) 由域 K 的单位元素 1 生成的子域是 K 的一切子域的交，因而是 K 的唯一的最小子域，称为素域．

2) 特征不同的素域彼此不同构．因此，特征不同的域互不同构．特征相同的域至少有一个共同的子域即素域．

3) 每个素域只有恒等自同构．

设 $\chi(K)=0$．$n\cdot a=0$ $(a\in K, n\in\mathbf{Z})$ 当且仅当 $a=0$ 或 $n=0$．对于一个素数特征的域 K 来说，设它的特征为素数 p．由于对任意元素 $a\in K$ 我们有 $p\cdot a=0$，应用二项式定理，对于任意元素 $a, b\in K$，不难证明下式成立

$$(a+b)^p=a^p+b^p. \tag{1}$$

这是因为上式左端按二项式定理展开

$$(a+b)^p=a^p+\begin{pmatrix}p\\1\end{pmatrix}a^{p-1}b+\cdots+\begin{pmatrix}p\\p-1\end{pmatrix}ab^{p-1}+b^p,$$

由于 p 为素数，所以 p 整除 $\begin{pmatrix}p\\i\end{pmatrix}$，$1\leq i\leq p-1$；从而上式右端中间各项全等于零，于是上式就变成 (1) 式．

(1) 还可推广成

$$\left(\sum_{i=1}^{r} a_i\right)^{p^s} = \sum_{i=1}^{r} a_i^{p^s}, \quad a_i \in K, i = 1, \cdots, r.$$

在 (1) 中将 b 换成 $b-a$ 得 $(b-a)^p = b^p - a^p$.

在 K 中任意取定一个子域 F 作为 **基域**,K 看作 F 上的扩域，叫做 F 上的 **域扩张**, 记作 K/F. K 的包含 F 的任一个子域叫做 K/F 的 **中间域**. 设 S 为 K 的一个非空子集， K 中包含 F 和 S 的一切子域的交记作 $F(S)$, 叫做在 F 上 **添加** S 得到的子域或叫做 S 在 F**上生成** 的子域. 用 $F[S]$ 表示下列一切有限和

$$\sum_{i_1,\cdots,i_n \geq 0} a_{i_1\cdots i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n}, \quad \alpha_1, \cdots, \alpha_n \in S$$

组成的集合，$F[S]$ 是 K 的一个子环，$F[S]$ 的商域就是 $F(S)$. 特别当 S 为有限子集 $\{\alpha_1, \cdots, \alpha_n\}$ 时，$F(S)$ 和 $F[S]$ 分别记成 $F(\alpha_1, \cdots, \alpha_n)$ 和 $F[\alpha_1, \cdots, \alpha_n]$, 显然 $F(\alpha_1, \cdots, \alpha_r, \beta_1, \cdots, \beta_s) = F(\alpha_1, \cdots, \alpha_r)(\beta_1, \cdots, \beta_s) = F(\beta_1, \cdots, \beta_s)(\alpha_1, \cdots, \alpha_r)$.

若 F 的域扩张 K 可以在 F 上添加一个元素 α 得到， $K = F(\alpha)$, 则 K 叫做 F 上的一个 **单扩张**.

下面的定理给出了单扩张的构造.

定理 1 *设 K/F 为一个域扩张， $\alpha \in K$. 于是*

1) 若 α 在 F 上是代数的，$f(x) \in F[x]$ 为 α 的极小多项式，则 $F(\alpha) = F[\alpha]$ 且 $F(\alpha) \cong F[x]/(f(x))$, $f(\alpha) = 0$ 是 α 在 F 上的唯一的基本关系;

2) 若 α 在 F 上是超越的，则 $F[\alpha] \cong F[x]$, 因而 $F(\alpha)$ 和 $F[x]$ 的商域 $F(x)$ 同构.

证明 根据第三章定理 14, 存在一个满同态 $\eta : F[x] \to F[\alpha]$ 使得 $\eta(x) = \alpha$, η 在 F 上为恒等同构，记 $I = \ker(\eta)$, 于是 $I = (f(x))$. 假定 $f(x)$ 的首项系数为 1(若 $f(x) \neq 0$). 若 α 在 F 上为代数元，则 $f(x) \neq 0$, $f(x)$ 为一个次数 > 0 的不可约多项式. 根据第三章定理 21,$F[x]/(f(x))$ 为一域. 因而 $F[\alpha]$ 已是一个域， $F[\alpha] = F(\alpha) \cong F[x]/(f(x))$, $f(x)$ 为 α 的极小多项式. 当 α 在 F 上为超越元时， $f(x) = 0$, $F[\alpha] \cong F[x]$, 所以 $F(\alpha)$ 和 $F[x]$ 的商域同构. □

定理 1 的 1) 和 2) 中的单扩张分别叫做 **单代数扩张** 和 **单超越扩张**. 考察一下单代数扩张 $F(\alpha)$ 的运算，设 $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$. 由 $f(\alpha) = 0$ 得

$$\alpha^n = -(a_1\alpha^{n-1} + \cdots + a_n) \tag{1}$$

因此 α^m, $m \geq n$, 经过 (1) 逐次叠代，恒可表成 $1, \alpha, \cdots, \alpha^{n-1}$ 的线性组合，因而 $F(\alpha)$ 的每个元素可以表成

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}, \quad b_i \in F, \tag{2}$$

而且表法唯一，元素相加按多项式加法相加，它的相乘，按多项式相乘，乘得的结果，利用 (1) 将 α 的高次幂 α^m, $m \geq n$ 逐次降低，使得结果最后表成 (2) 的形式.

定义 1 设 K_i/F, $i=1,2$, 为两个域扩张，若存在 K_1 到 K_2 的一个同构 (或同态)η, 使得 η 限制在 F 上为恒等同构，则 η 叫做一个 F-**同构**(或 F-**同态**).

设 $\eta: K/F \to K'/F$ 是一个 F- 同构， $\alpha \in K$, 则 α 在 F 上是代数的当且仅当 $\eta(\alpha)$ 在 F 上是代数的. 此时 α 和 $\eta(\alpha)$ 有相同的极小多项式.

替代代数基本定理的作用的有根的存在定理.

定理 2 *设 F 为一域， $P(x) \in F[x]$ 为一个不可约多项式，则存在一个域扩张 K/F 使得 $P(x)$ 在 K 内有根. 设 $F(\alpha_1)/F$ 和 $F(\alpha_2)/F$ 为两个单代数扩张，α_1, α_2 都是 $P(x)$ 的根，则 $F(\alpha_1)$ 和 $F(\alpha_2)$ 有一个 F- 同构 η 使得 $\eta(\alpha_1)=\alpha_2$.*

证明 因 $P(x)$ 不可约， $P(x)$ 在 $F[x]$ 内生成一个极大理想 $(P(x))$, 商环 $F[x]/(P(x))$ 为一域，记作 K, 映射 $a \mapsto \overline{a} = a + (P(x))$ 是 F 到 K 的一个单一同态，将 a 与 $\overline{a}$ 等同，于是 F 嵌入 K, 成为 K 的一个子域. 令 $\alpha = \overline{x} = x + (P(x))$, 令 $P(x) = a_0 + a_1 x + \cdots + x^n$, 于是有

$$P(\alpha) = a_0 + a_1\alpha + \cdots + \alpha^n = \overline{a}_0 + \overline{a}_1\overline{x} + \cdots + \overline{x}^n = \overline{P(x)} = \overline{0}.$$

所以 α 为 $P(x)$ 的一根，根据定理 1,1) 的证明， $F(\alpha_1)$ 和 $F(\alpha_2)$ 都 F- 同构于 $F[x]/(P(x))$ 而且 α_i 与 $\overline{x}$ 对应. 所以 $F(\alpha_1)$ 与 $F(\alpha_2)$ 成 F- 同构且 α_1 与 α_2 对应. □

§2 有限扩张

域 F 上的一个域扩张 K/F 叫做 **代数扩张**, 如果 K 的每个元素都是 F 上的代数元. 以后 F 上的域扩张也可简称为 F 上的扩张.

F 上的扩张 K 可以看作 F 上的一个线性空间， K 对 F 的维数叫做扩张 K/F 的 **次数**, 记作 $[K:F]$. 如果 $[K:F] < \infty$, 则 K/F 叫做 **有限扩张**. 否则，K/F 叫做 **无限扩张**.

设 K/F 为一有限扩张. 当 K 作为 F 上线性空间时， K 对 F 的一基也叫做扩张 K/F 的一 **基**.

设 $\alpha \in K$ 为 F 上一个代数元. α 的极小多项式 $f(x)$ 的次数叫做 α 的 **次数**.F 中元素的次数都为 1. 若 $\alpha \notin F$, 则 α 的次数 >1. α 的次数也可以如下来刻画：设 $f(x)$ 的次数为 n. 根据定理 1,1), 可知 F 上一个多项式 $g(x)$ 以 α 为根的充分必要条件是 $f(x)|g(x)$. 由此可知， $1, \alpha, \cdots, \alpha^{n-1}$ 在 F 上线性无关，

而 $1,\alpha,\cdots,\alpha^n$ 在 F 上线性相关. 因此 α 的次数 n 是使得 $1,\alpha,\cdots,\alpha^n$ 在 F 上线性相关的最小正整数.

一般说来, 元素 $\alpha\in K$ 在 F 上是代数的, 其充分必要条件是存在一个正次数的多项式 $g(x)\in F[x]$ 以 α 为根, 也就是存在一个正整数 m, 使得 $1,\alpha,\cdots,\alpha^m$ 在 F 上线性相关. 这就证明了

引理 1 *设 K/F 为一扩张, $\alpha\in K$, α 在 F 上是代数的其充分必要条件是存在一个正整数 m 使得 $1,\alpha,\cdots,\alpha^m$ 在 F 上线性相关. 若 α 为 F 上代数元, 则 α 的次数等于最小正整数 n 使得 $1,\alpha,\cdots,\alpha^n$ 在 F 上线性相关.* □

引理 2 *任一有限扩张 K/F 是一代数扩张.*

证明 设 $[K:F]=n$. 对每个 $\alpha\in K$, $1,\alpha,\cdots,\alpha^n$ 在 F 上线性相关, 所以 α 是 F 上代数元. □

定理 3 *设 K/F 为任一扩张, $\alpha\in K$, 则下列叙述是等价的:*

1) *$F(\alpha)/F$ 是代数扩张;*

2) *α 在 F 上是代数的;*

3) *$F(\alpha)/F$ 是有限扩张.*

当条件有一成立, 则 $[F(\alpha):F]$ 等于 α 的次数.

证明 1) ⇒ 2) 由代数扩张的定义即得.

2) ⇒ 3) 设 α 为 F 上一个 n 次代数元. 根据定理 1 下面的说明, $1,\alpha,\cdots,\alpha^{n-1}$ 是 $F(\alpha)/F$ 的一基. 因而 $[F(\alpha):F]=n$.

3) ⇒ 1) 即引理 2. □

定理 3 说明了, 为什么当 α 为 F 上代数元时, $F(\alpha)/F$ 叫做单代数扩张的理由.

定理 4 *设 $K\supset E\supset F$ 为 F 上的扩域, 则 $[K:F]$ 为有限的充要条件是 $[K:E]$ 和 $[E:F]$ 都有限. 在这种情况下有次数关系*

$$[K:F]=[K:E][E:F]. \tag{3}$$

证明 设 $[K:F]<\infty$. 由于 E/F 是 K/F 的子空间, 所以 $[E:F]\leq[K:F]$. 设 $\alpha_1,\cdots,\alpha_n$ 为线性空间 K 对 F 的一组基, 若把 K 看作 E 上的线性空间, 则 $\alpha_1,\cdots,\alpha_n$ 显然是 K/E 的一组生成元, 所以 $[K:E]\leq n=[K:F]$. 反之, 设 $[K:E]=m,[E:F]=r$ 都有限, 并设 $\beta_1,\cdots,\beta_m$ 和 $\gamma_1,\cdots,\gamma_r$ 分别是 K/E 和 E/F 的基. 于是对 $\alpha\in K$, α 可写成 β_i 的线性组合, 系数属于 E:

$$\alpha=\sum_{i=1}^m a_i\beta_i,\quad a_i\in E.$$

而 a_i 又可写成 γ_j 的线性组合，系数属于 F:

$$a_i = \sum_{j=1}^{r} b_{ij}\gamma_j, \quad b_{ij} \in F.$$

于是 α 可表成 $\beta_i\gamma_j$ 的线性组合，系数属于 F:

$$\alpha = \sum_i \left(\sum_j b_{ij}\gamma_j\right)\beta_i = \sum_{i,j} b_{ij}\beta_i\gamma_j, \quad b_{ij} \in F.$$

所以 $[K:F] \leq [K:E][E:F]$. 其次，证明 $\{\beta_i\gamma_j\}$ 在 F 上线性无关. 设

$$\sum_{i,j} b_{ij}\beta_i\gamma_j = 0, \quad b_{ij} \in F$$

为任一个线性关系，令 $a_i = \sum\limits_j b_{ij}\gamma_j$, $i = 1, \cdots, m$. 则 $a_i \in E$ 而且 $\sum a_i\beta_i = 0$. 由于 $\{\beta_i\}$ 为 K/E 的一基，从此推出所有 $a_i = 0$. 又因为 $\{\gamma_j\}$ 为 E/F 的一基，从 $a_i = \sum\limits_j b_{ij}\gamma_j = 0$ 推出所有 $b_{ij} = 0$. 所以 $\{\beta_i\gamma_j\}$ 在 F 上线性无关. 它们构成 K/F 的一基，所以

$$[K:F] = mr = [K:E][E:F]. \quad \square$$

设 K/F 为一有限扩张，E/F 为 K/F 的任一中间域，则 $[E:F] \leq [K:F]$，而且 $E = K$ 的充要条件是 $[E:F] = [K:F]$. 一个素数次扩张 K/F 除 K 和 F 外无其它中间域.

推论 1 每个有限扩张 K/F 有一个中间域的有限升链.

$$F = F_0 \subset F_1 \subset \cdots \subset F_r = K, \tag{4}$$

使得 F_{i+1}/F_i 为单代数扩张. (4)**叫做单代数扩张升链**. 反之，若 K/F 有一个单代数扩张有限升链，则 K/F 为有限扩张.

证明 证明推论的第一部分. 设 K/F 为有限扩张，对次数 $[K:F]$ 作归纳法. 取一个 $\alpha_1 \in K$ 但 $\alpha_1 \notin F$, 作 $F_1 = F(\alpha_1)$, 则 F_1/F 为单代数扩张且 $[F_1:F] > 1$. 从而 $[K:F_1] < [K:F]$, 根据归纳法假设，K/F_1 有一个单代数扩张升链 $F_1 \subset F_2 \subset \cdots \subset F_r = K$. 于是 $F \subset F_1 \subset F_2 \subset \cdots \subset F_r = K$ 就是 K/F 的一个单代数扩张升链. 推论的第二部分由定理 3 和 4 即得. $\square$

推论 2 设 $K \supset E \supset F$ 为 F 上扩张，若 K/E 和 E/F 都是代数扩张，则 K/F 也是代数扩张，特别，F 上的代数元 α, β 的和、差、积、商仍为 F 上代数元.

证明 设 $\alpha \in K$ 为任一元，因 α 在 E 上是代数的，α 在 E 上有正次数的极小多项式 $g(x) = x^r + a_1x^{r-1} + \cdots + a_r$, $a_i \in E$. 又因 E/F 是代数扩张，a_i 都是 F 上代数元. 令 $F_0 = F, F_i = F_0(a_1, \cdots, a_i)$, $i = 1, 2, \cdots, r, F_{r+1} = F_r(\alpha)$. 于是

$$F = F_0 \subset F_1 \subset \cdots \subset F_r \subset F_{r+1}$$

是单代数扩张升链. 由推论 1,F_{r+1}/F 为有限扩张. 因 $\alpha \in F_{r+1}$ 可知 α 是 F 上代数元. 所以 K/F 为代数扩张. 特别 $\alpha \pm \beta, \alpha \cdot \beta$ 和 α/β ($\beta \neq 0$) 都属于 $F(\alpha, \beta)$. 而且 $F(\alpha, \beta)/F(\alpha)$ 和 $F(\alpha)/F$ 都是代数扩张，所以 $\alpha \pm \beta, \alpha \cdot \beta$ 和 α/β 都是 F 上代数元. □

在任一域扩张 K/F 中 F 上的代数元全体构成一个中间域，叫做 F 在 K 中的 **代数闭包**. K 中任一不属于此代数闭包的元素在 F 上是超越的.

例 复数域 $\mathbf{C}$ 是有理数域 $\mathbf{Q}$ 上的域扩张. 如果复数 α 在 $\mathbf{Q}$ 上是代数的，则 α 叫做一个 **代数数**. 由推论 2 可知 $\mathbf{C}$ 中代数数全体，记作 $\overline{\mathbf{Q}}$, 对加、减、乘、除封闭，因而 $\overline{\mathbf{Q}}$ 是 $\mathbf{C}$ 的一个子域，叫做 **代数数域**. $\overline{\mathbf{Q}}$ 是 $\mathbf{Q}$ 在 $\mathbf{C}$ 中的代数闭包.

§3 分裂域、正规扩张

给定一个基域 F 和 $F[x]$ 的一个 n ($n \geq 1$) 次多项式 $f(x)$, 讨论 $f(x)$ 的根不仅是孤立地研究 $f(x)$ 的单个根，而且还要进一步研究 $f(x)$ 的诸根间在 F 上的代数关系，这就需要将 $f(x)$ 的全部根放在 F 的同一个域扩张中来考虑. 当 F 为有理数域时，根据历史上的代数基本定理，复数域可以充当这样的扩域. 但是当 F 为一个素数特征的域时，复数域则无能为力. 本节来研究这种扩张的存在性和唯一性.

定义 2 取定一个基域 F 和一个 n ($n \geq 1$) 次多项式 $f(x)$, 如果有一个域扩张 E/F 满足

1) $f(x)$ 在 E 内完全分解成一次因式的乘积

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_n), \quad \alpha_i \in E, \ i = 1, \cdots, n;$$

2) $E = F(\alpha_1, \cdots, \alpha_n)$;

则 E/F 叫做 $f(x)$ 的一个 **分裂域**.

定理 5 *每个正次数多项式 $f(x) \in F[x]$ 有一个分裂域.*

证明 对 $f(x)$ 的次数作归纳法. 当 $\deg f(x) = 1$ 时，$f(x) = c(x - \alpha)$, $\alpha \in F$, 显然 F 本身是 $f(x)$ 的一个分裂域. 假设当 $\deg f(x) < n$ ($n > 1$) 时 $f(x)$ 有一个分裂域. 求证当 $\deg f(x) = n$ 时，$f(x)$ 有一个分裂域. 任取 $f(x)$ 的一个不可约因式

$p(x)$, 根据定理 2, 存在一个单代数扩张 K_1/F 使得 $K_1 = F(\alpha_1), p(\alpha_1) = 0$. 于是 $p(x)$ 在 K_1 上析出一个一次因式, 因而 $f(x)$ 在 K_1 上至少析出一个一次因式. 可设 $f(x) = (x-\alpha_1)\cdots(x-\alpha_r)f_1(x), f_1(x) \in K_1[x], \alpha_i \in K_1, i = 1,\cdots,r, r \geq 1$. 此时 $\deg f_1(x) < n$, 若 $f_1(x)$ 为常数, 则 K_1/F 就是 $f(x)$ 的分裂域; 若 $\deg f_1(x) \geq 1$, 则根据归纳法假设, $f_1(x)$ 在 K_1 上有一个分裂域 E/K_1. 于是

$$f_1(x) = c(x-\alpha_{r+1})\cdots(x-\alpha_n),\ \ \alpha_i \in E,\ i = r+1,\cdots,n.$$

$$\begin{aligned}E&=K_1(\alpha_{r+1},\cdots,\alpha_n) = F(\alpha_1)(\alpha_{r+1},\cdots,\alpha_n)\\&=F(\alpha_1,\cdots.\alpha_r)(\alpha_{r+1},\cdots,\alpha_n) = F(\alpha_1,\cdots,\alpha_n).\end{aligned}$$

所以 E/F 就是 $f(x)$ 的一个分裂域. □

推论 设 $\deg f(x) = n$, 则分裂域 E/F 的次数不超过 $n!$.

其次证明分裂域的唯一性.

引理 1 设 $\sigma: F \to F'$ 是一个域同构, 又设 $F[x]$ 和 $F'[y]$ 分别为 F 和 F' 上一元多项式环, 则 σ 可以唯一地开拓成环同构 $\overline{\sigma}: F[x] \to F'[y]$, 使得 $\overline{\sigma}(x) = y$.

证明 根据第三章定理 14, 映射 σ 的开拓 $\overline{\sigma}: f(x) \mapsto f^\sigma(y)$

$$\begin{aligned}f(x) &= a_0 + \cdots + a_n x^n \in F[x],\\ f^\sigma(y) &= \sigma(a_0) + \cdots + \sigma(a_n)y^n\end{aligned}$$

是一个满同态 $F[x] \to F'[y], \overline{\sigma}(x) = y$, 而且唯一. 由于 y 是 F' 上未定元, $\ker(\overline{\sigma}) = (0)$, 因而 $\overline{\sigma}$ 是一个同构. □

为简单起见, 以后 $\sigma: F \to F'$ 在 $F[x]$ 到 $F'[y]$ 的开拓仍记作 σ. 在 σ 下 $F[x]$ 的不可约多项式和 $F'[y]$ 的不可约多项式相对应.

引理 2 设 $\sigma: F \to F'$ 为域同构, $F(\alpha)$ 和 $F'(\alpha')$ 为两个单代数扩张, α 和 α' 分别为 $F[x]$ 中不可约多项式 $p(x)$ 和 $F'[y]$ 中相应的不可约多项式 $p^\sigma(y)$ 的根. 则 σ 可唯一地开拓成同构 $\sigma': F(\alpha) \to F'(\alpha')$ 使得 $\sigma'(\alpha) = \alpha'$.

证明 首先 σ 开拓成环同构 $\sigma: F[x] \to F'[y]$. 于是 σ 诱导出环同构 $\sigma': F[x]/(p(x)) \to F'[y]/(p^\sigma(y))$. 根据定理 2, σ' 可以理解为同构 $F(\alpha) \to F'(\alpha')$ 使得 $\sigma'(\alpha) = \alpha'$ 而且 $\sigma'|_F = \sigma$. σ' 的唯一性显然. □

定理 6 设 $\sigma: F \to F'$ 为一个域同构, $f(x)$ 为 $F[x]$ 的一个正次数多项式, E 和 E' 分别为 $f(x)$ 和 $f^\sigma(x)$ 在 F 和 F' 上的分裂域, 则 σ 可以开拓成同构 $E \to E'$.

证明 对次数 $[E:F]$ 作归纳法. 当 $[E:F] = 1$ 时, $E = F(\alpha_1,\cdots,\alpha_n) = F$, 即 $f(x)$ 在 $F[x]$ 内完全分解 $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$, $\alpha_i \in F$, 在 σ 下 $f^\sigma(x) = c'(x-\alpha_1')\cdots(x-\alpha_n'), c' = \sigma(c), \alpha_i' = \sigma(\alpha_i)$, 从而 $\alpha_i' \in F', i = 1,\cdots,n$,

于是 $E' = F'(\alpha_1', \cdots, \alpha_n') = F'$. 定理对这种情况显然成立. 假设当 $[E:F] < n$ $(n > 1)$ 时, 定理成立. 进而证明定理当 $[E:F] = n$ 时也成立. 设 $[E:F] = n$, 由于 $n > 1, f(x)$ 有一个次数 > 1 的不可约因式 $p(x)$, 设 $\alpha \in E$ 为 $p(x)$ 的一根, $p^\sigma(x)$ 为 $f^\sigma(x)$ 的一个不可约因式, 设 α' 是 $p^\sigma(x)$ 在 E' 内的一根. 根据引理 2, 存在一个域同构 $\sigma_1 : F(\alpha) \to F'(\alpha')$, 它是 σ 的开拓, 而且 $\sigma_1(\alpha) = \alpha'$. 此时, $E/F(\alpha)$ 和 $E'/F'(\alpha')$ 分别是 $f(x)$ 和 $f^\sigma(x)$ 的分裂域. 由于 $[F(\alpha):F] > 1$, 根据定理 4 可知 $[E:F(\alpha)] < n$, 根据归纳法假设, σ_1 可以开拓成同构 $E \to E'$. 于是定理普遍成立. □

推论 *任意给定基域 F 和正次数多项式 $f(x) \in F[x]$, 则 $f(x)$ 在 F 上的任意两个分裂域 E, E' 成 F- 同构. 因而 $f(x)$ 在 F 上的分裂域在 F- 同构意义下是唯一的.* □

在这里指出关于分裂域的两个简单的事实. 第一, 若一个域扩张 K/F 含有两个中间域 E/F 和 E'/F. 它们是同一个多项式 $f(x) \in F[x]$ 的分裂域, 则 $E = E'$. 因为 $F(x)$ 在 E 内的分解 $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ 和在 E' 内的分解 $f(x) = c'(x-\alpha_1')\cdots(x-\alpha_n')$, 实质上它们都是 $f(x)$ 在 K 内的分解, 根据 $K[x]$ 的整除理论, 可知 $c = c', (x-\alpha_1), \cdots, (x-\alpha_n)$ 不过是 $(x-\alpha_1'), \cdots, (x-\alpha_n')$ 的一个排列. 所以 $E = E'$. 第二, 若扩张 K/F 的一个中间域 E/F 是一个多项式 $f(x) \in F[x]$ 的分裂域, 则 E 在 K 的任一个 F- 自同构 σ 下保持不变, 即 $\sigma(E) = E$. 这是因为 $\sigma(E)$ 是多项式 $f^\sigma(x)$ 的分裂域. 由于 $f(x) \in F[x], f^\sigma(x) = f(x)$. 由上可知 $\sigma(E) = E$.

将来就会看到, $f(x)$ 的诸根在 F 上的代数性质由它的分裂域 E/F 的代数性质反映出来.

分裂域有一个定性的刻画, 就是它的正规性.

定义 3 一个代数扩张 K/F 叫做 **正规扩张**, 如果 K/F 具有下列的性质: 若 $F[x]$ 的任一个不可约多项式在 K 内有一根, 则它在 K 内可以完全分解成一次因式的乘积.

定理 7 *一个有限扩张 K/F 是正规扩张的充要条件是 K 为 $F[x]$ 的一个多项式的分裂域.*

证明 设 K/F 为一有限正规扩张. 首先根据定理 4 的推论, K 可以写成 $K = F(\alpha_1, \cdots, \alpha_r)$, α_i 在 F 上为代数的. 设 $f_i(x)$ 为 α_i 在 F 上的极小多项式. 令 $f(x) = \prod_{i=1}^{r} f_i(x)$. 由于 K/F 正规, 每个 $f_i(x)$ 在 K 内完全分解成一次因式乘积, 因而 $f(x)$ 也是这样. 令 $f(x) = (x-\beta_1)\cdots(x-\beta_n)$, 于是 $\beta_i \in K, F(\beta_1, \cdots, \beta_n) \subset K$. 反之显然 $K \subset F(\beta_1, \cdots, \beta_n)$, 所以 $K = F(\beta_1, \cdots, \beta_n)$ 是 $f(x)$ 的分裂域.

反之, 设 K/F 为多项式 $f(x) \in F[x]$ 的一个分裂域, 设 $p(x)$ 为 $F[x]$ 的任一

个不可约多项式，而且在 K 内有一根 α. 求证 $p(x)$ 在 K 内完全分解. 设 E/K 是 $p(x)$ 在 K 上的分裂域，易见 E/F 就是 $g(x)=f(x)p(x)$ 在 F 上的分裂域. 设 β 为 $p(x)$ 在 E 内的任一根，则有一个 $F(\alpha)$ 到 $F(\beta)$ 的 F- 同构 τ 使得 $\tau(\alpha)=\beta$. 根据定理 6, τ 可以开拓成 E 的一个 F- 自同构 σ. 因为 K/F 是 $f(x)$ 的分裂域，根据上面的说明， $\sigma(K)\subset K$. 由于 $\alpha\in K$, 从而 $\beta=\tau(\alpha)\in K$. 因此 $p(x)$ 在 K 内完全分解. 这就证明了 K/F 正规. □

由定理 7 可知，若 E/F 是一个正规扩张，则对 E 的任一个中间域 L, E/L 也是正规扩张.

设 K/F 是一个有限扩张. 如果 K 上一个代数扩张 E/K 满足：

1) E/F 是正规扩张；

2) 若中间域 L $(F\subset L\subset E)$ 包含 K 而且 L/F 正规，则

$$L=E.$$

则 E/F 叫做 K/F 的一个 **正规闭包**.

首先证明正规闭包的存在. 将 K 写成 $K=F(\alpha_1,\cdots,\alpha_r)$, $f_i(x)$ 为 α_i 在 F 上的极小多项式. 令 $f(x)=\prod\limits_{i=1}^{r}f_i(x)$. 取 E 为 $f(x)$ 在 K 上的分裂域. 于是 E 是 $f(x)$ 在 F 上的一个分裂域，因而是 F 上的正规扩张而且包含 K. E 满足条件 2) 是显然的. 所以 E 是 K/F 的一个正规闭包. 其次证明 K/F 的正规闭包在同构意义下是唯一的. 设 E'/F 为 K/F 的任一个正规闭包. 因为每个 $f_i(x)$ 在 E' 内有根，因而在 E' 内完全分解，因而 $f(x)$ 在 E' 内也完全分解. 于是 E' 包含 $f(x)$ 在 F 上的一个分裂域 E_1. 由于条件 2) 从 $K\subset E_1\subset E'$ 推出 $E_1=E'$. 根据定理 6 的推论知 E' 是由 K/F 唯一决定的.

例 1 设 F 为域. $f(x)=x^2+ax+b\in F[x]$. 若 $f(x)$ 在 $F[x]$ 内可约，$f(x)=(x-c_1)(x-c_2)$, $c_i\in F$, 则 $F(c_1,c_2)=F$ 就是 $f(x)$ 的分裂域. 设 $f(x)$ 不可约. 作 $K=F[x]/(f(x))$, 令 $\alpha=x+(f(x))$, 于是 $K=F(\alpha)$. $f(x)$ 以 α 为根. $f(x)$ 的另一根 $\alpha'=-\alpha-a\in K$, 所以 $K=F(\alpha,\alpha')$ 为 $f(x)$ 的分裂域.

例 2 $F=\mathbf{Q}$, 有理数域. $f(x)=(x^2-2)(x^2-3)$. 首先 x^2-2 和 x^2-3 在 $\mathbf{Q}[x]$ 内都不可约，作 $K=\mathbf{Q}[x]/(x^2-2), \alpha=x+(x^2-2), K=\mathbf{Q}(\alpha)$ 是 x^2-2 的分裂域， $x^2-2=(x-\alpha)(x+\alpha)$. 其次 x^2-3 在 $K[x]$ 内不可约. 假若 x^2-3 在 $K[x]$ 内可约，则存在一个 $a+b\alpha\in K$ 使得 $(a+b\alpha)^2-3=a^2+\alpha^2b^2-3+2ab\alpha=a^2+2b^2-3+2ab\alpha=0$, 推出 $a^2+2b^2=3, ab=0$. 若 $a=0$, 则 $2b^2=3$, 但是不存在有理数 b 使得 $b^2=3/2$, 矛盾. 若 $b=0$, 则 $a^2=3$, 也不存在有理数 a 使得 $a^2=3$. 作 $E=K[x]/(x^2-3), \beta=x+(x^2-3)$, 于是 $E=K(\beta)=F(\alpha,\beta), f(x)=(x-\alpha)(x+\alpha)(x-\beta)(x+\beta)$, E 是 $f(x)$ 的分裂域，

$[E:\mathbf{Q}]=[E:K][K:\mathbf{Q}]=4$.

例 3 设 $F=\mathbf{Q}$, $f(x)=x^p-1$, p 为一素数. 首先 $f(x)=(x-1)p(x)$, $p(x)=x^{p-1}+x^{p-2}+\cdots+1$. 已知 $p(x)$ 在 $\mathbf{Q}$ 上不可约. 作 $K=\mathbf{Q}[x]/(p(x))$. 令 $\zeta=\overline{x}=x+(p(x))$. 于是 $K=\mathbf{Q}(\zeta)$, $\zeta^p=1$, $\zeta\neq 1$. 由于 p 为一素数, ζ 在 K 内生成一个 p 阶循环群 $\langle\zeta\rangle=\{1,\zeta,\cdots,\zeta^{p-1}\}$. 而且这 p 个元素恰好是 x^p-1 的全部根, 它们叫做 p 次单位根. 所以 $\mathbf{Q}(\zeta)=\mathbf{Q}(\zeta,\zeta^2,\cdots,\zeta^{p-1})$ 就是 x^p-1 的分裂域, 它的次数 $[\mathbf{Q}(\zeta):\mathbf{Q}]=p-1$.

例 4 设 $F=\mathbf{Q}, f(x)=x^p-2$, p 为素数. 首先 $f(x)$ 在 $\mathbf{Q}$ 上不可约. 作 $K=\mathbf{Q}[x]/(f(x))$, 令 $\alpha=\overline{x}=x+(f(x))$. 于是 $K=\mathbf{Q}(\alpha),\alpha^p-2=0$. 次数 $[K:\mathbf{Q}]=p$. $f(x)$ 在 K 上有分解 $f(x)=(x-\alpha)f_1(x), f_1(x)\in K[x]$, $\deg f_1(x)=p-1$. 下面将看出 $f_1(x)$ 在 K 上是不可约的, 不过暂时还不知道. 设 $p(x)$ 为 $f_1(x)$ 在 K 上的一个不可约因式, 作 $E=K[x]/(p(x))$, 令 $\beta=x+(p(x))$. 于是 $E=K(\beta)=\mathbf{Q}(\alpha,\beta)$, 注意 β 也是 $f(x)$ 的一根, $\beta^p-2=0$ 但 $\beta\neq\alpha$. 令 $\zeta=\beta/\alpha$, 于是 $\zeta\neq 1$ 而且 $\zeta^p=1$. ζ 是一个 p 次单位根. 由于 α,β 和 α,ζ 可以互相表出, 有 $E=\mathbf{Q}(\alpha,\beta)=\mathbf{Q}(\alpha,\zeta)$. 如例 3, ζ 在 E 内生成一个 p 阶循环群 $\langle\zeta\rangle=\{1,\zeta,\cdots,\zeta^{p-1}\}$. 那么 $\alpha,\zeta\alpha,\cdots,\zeta^{p-1}\alpha$ 就是 x^p-2 的全部根且都属于 E. 所以 E 是 x^p-2 的分裂域. 最后决定次数 $[E:\mathbf{Q}]$. 由 E 的构造知 $[E:\mathbf{Q}]=[E:K][K:\mathbf{Q}]\leq(p-1)p$. 另一方面, 由定理 4 和 $[K:\mathbf{Q}]=p$, 知 $p|[E:\mathbf{Q}]$. 由例 3 知 $[\mathbf{Q}(\zeta):\mathbf{Q}]=p-1$, 从而 $p-1|[E:\mathbf{Q}]$, p 与 $p-1$ 互素, 于是 $(p-1)p|[E:\mathbf{Q}]$. 最后得 $[E:\mathbf{Q}]=(p-1)p$. 由此可知 $\deg p(x)=p-1$, 从而 $p(x)=f_1(x)$. 如果将 E 看作复数域的子域, 则 α 可取 x^p-2 的唯一的正实根 $\sqrt[p]{2}$, (当 $p>2$ 时 x^p-2 只有一个实根) 而 β 可取 $e^{\frac{2\pi i}{p}}$.

§4 可分扩张

前面三节得到的结果与域的特征无关, 这一节引进的概念则和域的特征密切相关. 首先遇到的是根的重数问题.

域 F 上任一个正次数多项式 $f(x)$ 在它的分裂域 K 内可以唯一地写成

$$f(x)=c(x-\alpha_1)^{e_1}\cdots(x-\alpha_r)^{e_r},\quad e_i\geq 1.$$

其中 $\alpha_1,\cdots,\alpha_r\in K$ 两两不同. 这种分解与分裂域的选择无关, 就是说, 如果 $\overline{K}/F$ 为 $f(x)$ 的任一个分裂域, 则存在 K 到 $\overline{K}$ 的一个 F- 同构 $\alpha\mapsto\overline{\alpha}$ 使得 $f(x)$ 在 $\overline{K}$ 内有分解式

$$f(x)=c(x-\overline{\alpha}_1)^{e_1}\cdots(x-\overline{\alpha}_r)^{e_r},$$

而且 $\overline{\alpha}_i \neq \overline{\alpha}_j, i \neq j$. 因而这些指数 e_i 与分裂域的选择无关. α_i 叫做 $f(x)$**在 K 内的 e_i 重根**, 当 $e_i = 1$ 时, α_i 叫做 **单根**. 若 $e_i > 1$, 则 α_i 叫做 **重根**.

为了判断一个根是否是重根, 我们引进多项式的形式微商. 设 $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$, 系数属于一个域, 定义 $f(x)$ 的形式微商 $f'(x)$ 为

$$f'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + \cdots + a_{n-1}.$$

这个定义与系数所属的域没有关系. 形式微商有如下的基本性质:

1) $(f(x) + g(x))' = f'(x) + g'(x)$;

2) $(af(x))' = af'(x)$;

3) $(f(x) \cdot g(x))' = f'(x)g(x) + f(x)g'(x)$;

4) $x' = 1$.

这些性质在这里就不一一证明了. 其实 1),2),4) 是极其明显的, 只需证明 3). 对 $f(x)$ 的次数作归纳法, 当 $f(x)$ 为常数 a 时, 3) 即 2). 假设当 $\deg f(x) < n$ 时 3) 成立, 直接验算可知, $(x^{m+n})' = (x^m)'x^n + x^m(x^n)'$, 从而

$$(ax^n \cdot g(x))' = (ax^n)'g(x) + ax^ng'(x).$$

由于 $f(x)$ 可写成 $f(x) = ax^n + f_1(x), \deg f_1(x) < n$, 于是由归纳法假设, 有

$$\begin{aligned}(f(x) \cdot g(x))' &= (ax^ng(x) + f_1(x)g(x))' \\ &= (ax^ng(x))' + (f_1(x)g(x))' \\ &= (ax^n)'g(x) + ax^ng'(x) + f_1'(x)g(x) + f_1(x)g'(x) \\ &= f'(x)g(x) + f(x)g'(x).\end{aligned}$$

引理 1 设 $f(x) \in F[x]$, $x = \alpha$ 是 $f(x)$ 在它的分裂域 K 内的一个 k 重根, $k \geq 1$. 于是

1) 若 $\chi(F) \nmid k$, 则 $x = \alpha$ 是 $f'(x)$ 的 $k-1$ 重根. (当 $k = 1$ 时, 0 重根意即 $f'(\alpha) \neq 0$.)

2) 若 $\chi(F) | k$, 则 $x = \alpha$ 至少是 $f'(x)$ 的 k 重根.

证明 在 K 内 $f(x) = (x-\alpha)^k \cdot g(x), g(\alpha) \neq 0$, 于是

$$\begin{aligned}f'(x) &= k(x-\alpha)^{k-1}g(x) + (x-\alpha)^kg'(x) \\ &= (x-\alpha)^{k-1}(kg(x) + (x-\alpha)g'(x)) \\ &= (x-\alpha)^{k-1}q(x), \\ q(x) &= kg(x) + (x-\alpha)g'(x).\end{aligned}$$

若 $\chi(F) \nmid k$, 则 $k \neq 0$(在 K 内),$(x-\alpha) \nmid q(x)$, 所以 $x = \alpha$ 是 $f'(x)$ 的 $k-1$ 重根. 若 $\chi(F) | k$, 则 $k = 0$(在 K 内), 此时, $f'(x) = (x-\alpha)^kg'(x)$, $x = \alpha$ 至少是 $f'(x)$ 的 k 重根. □

定理 8 $F[x]$ 内一个正次数多项式 $f(x)$ 在它的分裂域 K 内无重根的充要条件是 $(f(x), f'(x)) = 1$.

证明 设 $f(x)$ 在 K 内无重根，则 $f(x)$ 在 K 内的每个根 α 都是单根. 无论 $\chi(F) = 0$ 或 $p > 0$, 总有 $\chi(F) \nmid 1$. 根据引理 1, α 不是 $f'(x)$ 的根. 设 $(f(x), f'(x)) = d(x)$, 则 $d(x) = 1$, 因为否则 $d(x)$ 在 K 内的根将是 $f(x)$ 和 $f'(x)$ 的公根. 反之，设 $f(x)$ 在 K 内有一个 k 重根， $k > 1$. 根据引理 1,α 至少是 $f'(x)$ 的 $k-1$ 重根， $k-1>0$, 因而 α 是 $(f(x), f'(x)) = d(x)$ 的根， $d(x)$ 非常数，所以 $f(x), f'(x)$ 不互素. □

推论 1 $F[x]$ 内一个不可约多项式 $p(x)$ 在它的分裂域内有重根的充要条件是 $p'(x) = 0$.

证明 根据定理 8, $p(x)$ 在 K 内有重根的充要条件是 $(p(x), p'(x)) = d(x)$ 非常数，由于 $p(x)$ 在 F 内不可约， $d(x) = p(x)$, 从而 $p(x) | p'(x)$, 但是 $p'(x)$ 的次数比 $p(x)$ 低，所以 $p'(x) = 0$. □

推论 2 若 $\chi(F) = 0$, 则 $F[x]$ 内任一不可约多项式在它的分裂域内只有单根.

证明 因为任一不可约多项式 $p(x)$ 的次数 > 0, 设 $p(x) = x^r + a_1x^{r-1} + \cdots + a_r \in F[x], r > 0$, 于是 $p'(x) = rx^{r-1} + (r-1)a_1x^{r-2} + \cdots + a_{r-1}$, 因为 $\chi(F) = 0$, 在 F 内 $r \neq 0$. 因而 $p'(x) \neq 0$, 根据推论 1, $p(x)$ 在它的分裂域内只有单根. □

当 F 的特征是一个素数时， F 上的不可约多项式是否有重根？为此我们引进可分多项式的概念.

定义 4 $F[x]$ 内一个不可约多项式 $p(x)$ 叫做 F 上的 **可分多项式**, 如果 $p(x)$ 在它的分裂域内只有单根. 任一个非常数多项式 $f(x) \in F[x]$ 叫做在 F 上可分的，如果它的每个不可约因式 (在 $F[x]$ 内) 都是可分的. 否则 $f(x)$ 叫做 F 上 **不可分多项式**.

设 K/F 为任一代数扩张， $\alpha \in K$ 叫做 F 上 **可分元素**, 如果 α 的极小多项式是 F 上可分多项式. 否则 α 叫做 F 上 **不可分元素**.

一个代数扩张 K/F 叫做 **可分扩张**, 如果 K 的每个元素在 K 上都是可分的. 否则 K/F 叫做 **不可分扩张**.

根据推论 2, 在特征 0 的域上不可约多项式都是可分的，因而特征 0 的域上任何代数扩张都是可分扩张. 下面来考查特征为素数的域上不可约多项式为不可分的情况. 设 $\chi(F) = p$(素数),$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ 为 F 上一个不可约多项式. 假设 $f(x)$ 为不可分，于是 $f'(x) = 0, ka_k = 0, k = 1, 2, \cdots, n$. 当 $p \nmid k$ 时，必须 $a_k = 0$, 因而 $f(x)$ 可写成 $a_0 + a_px^p + a_{2p}x^{2p} + \cdots + a_{mp}x^{mp}$. 令 $g(x) = a_0 + a_px + \cdots + a_{mp}x^m$, 则 $f(x) = g(x^p)$, $g(x)$ 必定在 F 上不可约，如果 $g(x)$ 不可分，则 $g(x)$ 又可写成 $g(x) = h(x^p)$ 而 $h(x)$ 在 F 上不可约，于是

$f(x)=h(x^{p^2})$. 这样 $f(x)$ 最终可写成

$$f(x)=\psi(x^{p^e}),\quad e\geq 1,$$

$\psi(x)$ 在 F 上是可分的. 进一步考查 $f(x)$ 在它的分裂域内的分解. 首先 $\psi(x)$ 可分解成 $\psi(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_r),\alpha_i\neq\alpha_j$, 于是 $f(x)=\prod_{i=1}^{r}(x^{p^e}-\alpha_i)$, 令 β_i 为 $x^{p^e}-\alpha_i$ 的一根, 注意在特征 p 的域内恒有等式 $(\alpha+\beta)^p=\alpha^p+\beta^p$, 于是

$$x^{p^e}-\alpha_i=x^{p^e}-\beta_i^{p^e}=(x-\beta_i)^{p^e},$$

于是得到 $f(x)$ 的最后分解式

$$f(x)=\prod(x^{p^e}-\alpha_i)=\prod(x^{p^e}-\beta_i^{p^e})=\prod(x-\beta_i)^{p^e}.$$

因此在特征 p 的域上一个不可分的不可约多项式的每个根有相同的重数, 其重数为 p 的一个方幂.

下面举一例说明确实存在不可分的不可约多项式. 令 $\mathbf{F}_p=\mathbf{Z}/(p),\mathbf{F}_p(t)$ 为一元多项式环 $\mathbf{F}_p[t]$ 的商域, 令 $F=\mathbf{F}_p(t)$, F 作为我们的基域, 在 $F[x]$ 内取 $f(x)=x^p-t$, 为了说明 $f(x)$ 在 F 上不可约, 我们需要

引理 2 *设 F 为一特征 p(素数) 的域, $a\in F$, 则 x^p-a 在 F 上不可约或者完全分解成 $x^p-a=(x-b)^p,b\in F$.*

证明 若 a 在 F 内可开 p 次方, 即 $a=b^p,b\in F$, 则 $x^p-a=x^p-b^p=(x-b)^p$. 假设 a 在 F 内不能开 p 次方, 证明 x^p-a 在 F 上不可约. 假设 x^p-a 在 $F[x]$ 内分解成 $x^p-a=f(x)\cdot g(x)$, $f(x)$ 的次数 r 适合 $1\leq r<p$, 把这个分解拿到 x^p-a 的分裂域 K 内去考虑, 设 α 为 x^p-a 在 K 内一根, 于是 $x^p-a=x^p-\alpha^p=(x-\alpha)^p=f(x)g(x)$, 从而 $f(x)=(x-\alpha)^r=x^r+\cdots+(-1)^r\alpha^r\in F[x],\alpha^r\in F$. 但是 $\alpha^p=a\in F$, 且 $(r,p)=1$, 令 $ur+vp=1$, 于是 $\alpha=\alpha^{ur+vp}=(\alpha^r)^u a^v\in F$, a 将在 F 内可开 p 次方, 矛盾. □

再回到 $f(x)=x^p-t$, t 在 $F=\mathbf{F}_p(t)$ 内不能开 p 次方. 因为, 若存在一个 $b=h(t)/g(t)$, $h(t),g(t)\in\mathbf{F}_p[t]$ 使得 $b^p=t$, 注意 $\mathbf{F}_p$ 的元素适合 $a^p=a$, 于是

$$t=b^p=(h(t)/g(t))^p=h(t)^p/g(t)^p=h(t^p)/g(t^p).$$

将有 $tg(t^p)=h(t^p)\neq 0$, 这在 $\mathbf{F}_p[t]$ 内不可能成立, 所以 x^p-t 在 F 上不可约. 由于 $(x^p-t)'=px^{p-1}=0$, 所以 x^p-t 在 F 上是不可分的.

这一节的后部分讨论嵌入与可分性的关系问题.

设 K/F 为一个有限扩张, E/F 为一个包含 K 的任意正规扩张. 设 L/F 为 K/F 的任一中间域. 如果一个同态 $\tau:L\to E$ 保持 F 的元素不动, 则 τ 叫

做 L 到 E 的一个 F- 嵌入即 F- 同态. 对于 K/F 的任意两个中间域 L_1, L_2, 若 $L_1 \subset L_2$ 而且 L_2 到 E 的 F- 嵌入 τ_2 限制在 L_1 上等于 L_1 到 E 的 F- 嵌入 τ_1, 则 τ_2 叫做 τ_1 在 L_2 上的一个开拓. 对于 K/F 的中间域 L 的一个 F- 嵌入 τ 和一个在 L 上的不可约多项式 $g(x)$, 若 $g(x)$ 在 K 内有一根 α, 则 $g(x)$ 在 τ 下的象 $g^{\tau}(x)$ 在 E 内就完全分解成一次因式的乘积. 这是因为, 设 $f(x) \in F[x]$ 为 α 在 F 上的极小多项式. 由于 E 包含 K 而且在 F 上正规, $f(x)$ 在 E 内就完全分解成一次因式的乘积. 另一方面, $g(x)$ 与 $f(x)$ 有公根 α, $g(x)$ 在 L 上不可约, 于是 $g(x)|f(x)$, $f(x) = g(x)\cdot h(x), h(x) \in L[x]$. 作用 τ, $f(x) = g^{\tau}(x)h^{\tau}(x)$, 从而 $g^{\tau}(x)|f(x)$. 所以 $g^{\tau}(x)$ 在 E 内也完全分解成一次因式的乘积.

引理 3 设 K/F 为一有限扩张, E/F 为包含 K 的任一正规扩张. L/F 为 K/F 的一个中间域, $\tau: L \to E$ 是一个 F- 嵌入, $\alpha \in K$ 为任意元素. 则 τ 在 $L(\alpha)$ 上的不同的开拓数 $N(\tau, L(\alpha))$ 等于 α 的极小多项式的不同根的个数. 因而 $N(\tau, L(\alpha)) \leq [L(\alpha):L]$. 等号成立当且仅当 α 是 L 上可分元.

证明 设 $g(x)$ 为 α 在 L 上的极小多项式. 根据上面的说明, $g^{\tau}(x)$ 在 E 内完全分解成一次因式的乘积: $g^{\tau}(x) = (x-\beta_1)\cdots(x-\beta_r), r = [L(\alpha):L]$. τ 在 $L(\alpha)$ 上任一开拓 σ 将 α 映到 $g^{\tau}(x)$ 的一根 $\sigma(\alpha)$, σ 由 α 的象 $\sigma(\alpha)$ 唯一决定. 因而不同的开拓将 α 映到不同的根. 反之, 对 $g^{\tau}(x)$ 的任一根 β, 根据本章 §3 引理 2, 存在 τ 的一个开拓 σ 使得 $\sigma(\alpha) = \beta$. 这样得到 τ 在 $L(\alpha)$ 上的开拓数 $N(\tau, L(\alpha))$ 等于 $g^{\tau}(x)$ 的相异根的个数, 也就是 $g(x)$ 的相异根的个数, 记作 r_0. 显然, $r_0 \leq r$. 等号成立当且仅当 $g(x)$ 是 L 上可分多项式即 α 是 L 上可分元. □

说明 τ 在 $L(\alpha)$ 上的开拓数 $N(\tau, L(\alpha))$ 只与 α 有关, 与 τ 的选取无关. 因此 $N(\tau, L(\alpha))$ 等于 $L(\alpha)$ 的 L- 嵌入数. 即 $\tau = 1$ 的情况.

定理 9 设 K/F 为一个有限扩张, E/F 为包含 K 的正规扩张. 则 K 到 E 内的 F- 嵌入数 $\leq [K:F]$. 等号成立当而且仅当 K/F 是可分扩张.

证明 有限扩张 K/F 可写成 $K = F(\alpha_1, \cdots, \alpha_r)$. 令 $F_0 = F, F_1 = F_0(\alpha_1), \cdots, F_r = F_{r-1}(\alpha_r) = K$, F_{i-1} 到 E 的任一 F- 嵌入 τ_{i-1} 在 F_i 上的开拓数记作 $N(F_{i-1}, F_i)$. 由引理 3 下面的说明, 这个数与 τ_{i-1} 的选取无关. 首先证明

$$N(F_0, F_1)N(F_1, F_2)\cdots N(F_{r-1}, F_r) = N(F, K). \tag{1}$$

$N(F, K)$ 表示 K 到 E 的 F- 嵌入数. 对 r 作归纳法. 当 $r = 1$ 时, 显然. 假设当生成元的个数小于 r 时成立. 求证生成元的个数为 r 时成立. 由归纳法假设有

$$N(F_0, F_1)\cdots N(F_{r-2}, F_{r-1}) = N(F, F_{r-1}).$$

根据引理 3, F_{r-1} 的每个 F- 嵌入在 K 上可开拓成 $N(F_{r-1}, F_r)$ 个 K 的 F-

嵌入，而且 K 的任一个 F- 嵌入必是 F_{r-1} 的某个 F- 嵌入的开拓. 因而有 $N(F,F_{r-1})N(F_{r-1},F_r)=N(F,K)$. 与上式联合得到 (1). 再根据引理 3, 有

$$N(F_{i-1},F_i)\le[F_i:F_{i-1}],\quad i=1,2,\cdots,r. \tag{2}$$

由 (1),(2) 以及域的次数公式就得

$$N(F,K)\le[K:F]. \tag{3}$$

其次证明定理的第二部分, 假设 K 在 F 上可分. 则每个 α_i 是 F 上可分元, 当然也是 F_{i-1} 上的可分元. 根据引理 3, (2) 中对 $i=1,\cdots,r$ 都取等号, 从而由 (1) 可知 (3) 中的等号成立. 反之，假设 K/F 是不可分扩张. 设 $\alpha\in K$ 是 F 上一个不可分元. 那么取 $\alpha_1=\alpha$ 作为第一个生成元. 根据引理 3, 有 $N(F_0,F_1)<[F_1:F_0]$, 从而得 $N(F,K)<[K:F]$. 这样就证明了定理的第二部分. □

推论 设 E/F 为有限正规扩张，G 为 E 的全部 F- 自同构组成的群，则 $|G|\le[E:F]$. 等号成立当且仅当 E/F 是可分扩张.

证明 在定理 9 中令 $K=E$. 对于 E 到自身的任一个 F- 嵌入 σ 有 $[\sigma(E):F]=[E:F]$, 从而 $\sigma(E)=E$. 因而 σ 是一个 F- 自同构. 反之显然. □

定理 10 设 L 为有限扩张 K/F 的任一中间域，则 K/F 是可分扩张当且仅当 K/L 和 L/F 都是可分的.

证明 必要性显然. 证充分性. 设 K/L 和 L/F 为可分扩张. 根据定理 9 的第一部分的证明，可知嵌入数有等式 $N(F,K)=N(F,L)N(L,K)$. 因为 K/L 和 L/F 都可分，根据定理 9, 有 $N(L,K)=[K:L]$ 和 $N(F,L)=[L:F]$. 由域的次数公式即得 $N(F,K)=[K:F]$. 再由定理 9 可知 K/F 是可分的. □

说明 定理 10 不限于有限扩张，对代数扩张也成立. 读者自己证明之.

由定理 10 不难证明

推论 1 在代数扩张 K/F 中可分元素的和、差、积、商 (0 不作除数) 都是可分的. □

推论 2 一个可分多项式的分裂域是可分的. □

推论 2 与定理 7 联合得到

定理 11 一个有限扩张 E/F 是可分正规的充要条件是 E 是 F 上一个可分多项式的分裂域. □

设 K/F 为任一代数扩张，K_s 表示 K 中全部可分元素组成的集合. 根据推论 1,K_s 是 K 的一个中间域，叫做 F 在 K 中的 **可分闭包**. 当特征 $\chi(F)=0$ 时，$K_s=K$; 当 $\chi(F)=$ 素数 p 时，K_s 有可能小于 K. 设 $K\ne K_s$. 对于任一 $\alpha\in K$, α 在 K_s 上的极小多项式 $f(x)$ 可写成 $f(x)=g(x^{p^e}),g(x)\in K_s[x]$ 为一

个 r 次不可约可分多项式. $g(x)$ 必须是一次的. 因为 $\beta=\alpha^{p^e}$ 是 $g(x)$ 的根, 因而 β 在 K_s 上可分. 根据定理 10 及其说明, β 是 F 上可分元, β 属于 K_s. 因而 $g(x)$ 是一次的, $g(x)=x-\beta$. 于是 $f(x)=x^{p^e}-\beta$. 当 $\alpha\notin K_s$ 时, $e\geq 1$, α 的 p^e 次幂落入 K_s. 这种元素叫做 K_s 上 **纯不可分元**, $f(x)=x^{p^e}-\beta$ 叫做 K_s 上 **纯不可分多项式**,K 叫做 K_s 上 **纯不可分扩张**.

§5 有限域

有限域又叫做 **伽罗瓦域**. 是由伽罗瓦首先提出而得名的. 有限域的特征显然只能是素数. 它是一类很重要的域, 它有很好的性质而且还有很重要的应用. 在第一章中对每个素数 p 已经给出一个特征 p 的域, 即整数模 p 的剩余类域 $\mathbf{F}_p=\mathbf{Z}/(p)$. 在这一节应用分裂域的结果对每个素数 p, 我们将给出全部特征 p 的有限域.

设 K 为一个特征 p 的有限域. 于是 K 包含 $\mathbf{F}_p$ 作为子域. K 自然地可以看成 $\mathbf{F}_p$ 上的有限维线性空间. 设 K 对 $\mathbf{F}_p$ 的维数为 n, $u_1,\cdots,u_n$ 为它的一基. 于是 K 的每个元素 α 可以唯一地表成 $u_1,\cdots,u_n$ 的线性组合

$$\alpha=a_1u_1+\cdots+a_nu_n,\quad a_i\in\mathbf{F}_p.$$

$a_1,\cdots,a_n$ 可以独立地取 $0,1,\cdots,p-1$. 因而 K 恰由 p^n 个元素组成. 因而这对 K 的基数作出了规定. K 的基数只能是它的特征的一个方幂, 幂指数等于 K 对 $\mathbf{F}_p$ 的维数, 也是 K 对 $\mathbf{F}_p$ 的次数.

其次, K 的全部非零元素 K^* 组成一个 p^n-1 阶乘法群. 根据拉格朗日定理, K^* 的每个元素都是方程 $x^{p^n-1}=1$ 的根, 因而 K 的每个元素都是 $x^{p^n}-x=0$ 的根. 但是 $x^{p^n}-x=0$ 在 K 内最多有 p^n 个根, 所以 K 的元素恰好是 $x^{p^n}-x$ 的全部根. 由于 $\mathbf{F}_p\subset K$ 可知 K 是 $x^{p^n}-x$ 在 $\mathbf{F}_p$ 上的分裂域. 这就证明下列定理的唯一性部分.

定理 12 *对每个素数 p 和任一正整数 n, 存在一个唯一的 p^n 个元素的有限域, 它就是 $x^{p^n}-x$ 在 $\mathbf{F}_p$ 上的分裂域. 除此之外无其它 p^n 个元素的有限域.*

证明 设 E 是 $x^{p^n}-x$ 在 $\mathbf{F}_p$ 上的分裂域. 首先证明 $x^{p^n}-x$ 在 E 内有 p^n 个不同的根. 由于微商 $(x^{p^n}-x)'=p^nx^{p^n-1}-1=-1$, 且 $-1\neq 0$, 所以 $x^{p^n}-x$ 只有单根. 于是 $x^{p^n}-x$ 在 E 内有 $p^n=q$ 个不同的根, 设为 $\alpha_1,\cdots,\alpha_q$. 令 $K=\{\alpha_1,\cdots,\alpha_q\}$. 证明 K 是 E 的一个子域. 对于 $\alpha,\beta\in K$, 有 $\alpha^{p^n}=\alpha,\beta^{p^n}=\beta$, 于是

$$(\alpha-\beta)^{p^n}=\alpha-\beta,$$
$$\left(\frac{\alpha}{\beta}\right)^{p^n}=\frac{\alpha^{p^n}}{\beta^{p^n}}=\frac{\alpha}{\beta},\quad \beta\neq 0.$$

从而 $\alpha-\beta, \dfrac{\alpha}{\beta}$ $(\beta\neq 0)$ 属于 K, 显然 $0,1\in K$. 所以 K 是 E 的子域. 而且 K 是 p^n 个元素的有限域. 这就证明了定理的存在性部分. 至于 $K=E$ 则是显然的. □

p^n 个元素的有限域习惯记成 $GF(p^n)$ 或 $\mathrm{F}_q, q=p^n$.

最后指出有限域 $GF(p^n)$ 有一个很重要的自同构即弗罗贝尼乌斯 (Frobenius) 自同构. 利用特征 $p>0$ 的域的一条性质 $(a+b)^p=a^p+b^p$, 作一个 $GF(p^n)$ 到自身的映射 $\sigma: x\mapsto x^p$. σ 满足

$$\begin{aligned}\sigma(x+y)&=(x+y)^p=x^p+y^p=\sigma(x)+\sigma(y),\\ \sigma(x\cdot y)&=(x\cdot y)^p=\sigma(x)\cdot\sigma(y).\end{aligned}$$

因而 σ 是一个自同态. 其次, σ 是单的. 这是因为 $\sigma(1)=1, 1\notin\ker(\sigma)$, 所以 $\ker(\sigma)=\{0\}$, 即 σ 单. 由于 $GF(p^n)$ 有限, 单射必然是满的. 所以 σ 是 $GF(p^n)$ 的一个自同构. 它叫做 $GF(p^n)$ 的弗罗贝尼乌斯**自同构**. σ 显然保持 $\mathbf{F}_p$ 的元素不动, 因而 σ 是一个 $\mathbf{F}_p$- 自同构.

作为弗罗贝尼乌斯自同构的一个推论, $GF(p^n)$ 的每个元素 a 可以开 p 次方. 因为 σ 是满射, a 在 σ 下有一个原象 b: $\sigma(b)=a$, 即 $b^p=a$, 所以 b 是 a 的一个 p 次方根. 由于 σ 的单一性, a 的 p 次方根是唯一的.

§6 分圆域

设 P 是一个素域. 就是说, 当特征 $\chi(P)=0$ 时, $P=\mathbf{Q}$, 有理数域; 当 $\chi(P)=p$ 素数时, $P=\mathbf{F}_p$, p 个元素的域. 设 n 为正整数. 这一节的目的是讨论 x^n-1 在 P 上的分裂域 E, 主要决定次数 $[E:P]$. 当 $\chi(P)=$ 素数 p 而且 $p|n$ 时, n 可写成 $n=p^r n', (n',p)=1$. 此时 $x^n-1=(x^{n'}-1)^{p^r}, x^n-1$ 和 $x^{n'}-1$ 在 P 上有相同的分裂域. 因此, 当 $\chi(P)=$ 素数时, 总是假定 $(n,p)=1$.

首先, 因为微商 $(x^n-1)'=nx^{n-1}\neq 0$, 它与 x^n-1 互素, x^n-1 在分裂域 E 中只有单根. 因而 x^n-1 在 E 内有 n 个不同的根, 每个根 ζ 适合 $\zeta^n=1$, ζ 叫做一个 n **次单位根**. 这 n 个 n 次单位根在 E 内形成一个乘法群, 记作 G. G 叫做 n 次单位根群. 根据第三章 §7 定理 19 可知 G 是一个循环群. G 的每个生成元叫做**本原 n 次单位根**. 设 ζ 为一个本原 n 次单位根, 则 $G=\{1,\zeta,\zeta^2,\cdots,\zeta^{n-1}\}$, 而且 ζ^ν 为 n 次本原单位根当而且仅当 $(\nu,n)=1$. 因而 n 次本原单位根有 $\varphi(n)$ 个, $\varphi(n)$ 为欧拉函数. 本原 n 次单位根不能是任何 x^d-1 的根, 其中 $d|n$ 且 $d<n$.

其次, x^n-1 的分裂域 E 是由它的全部根在 P 上生成的, 实际上 E 可由一个本原 n 次单位根 ζ 生成, 因而 E 是 P 上的一个单扩张, $E=P(\zeta)$. 最后

来确定 E/P 的次数. 分两种情况讨论.

1) $\chi(P)=$ 素数 p, 此时 $P=\mathbf{F}_p$, $(n,p)=1$. 设 $[E:\mathbf{F}_p]=r$, 由 §4 可知, E 是 p^r 个元素的有限域, $E=GF(p^r)$. 设 e 为 $p \bmod n$ 的指数, 即最小正整数 e 使得 $p^e\equiv 1(\mathrm{mod}\ n)$. 我们求证 $e=r$. 一方面乘法群 E^* 是一个 p^r-1 阶群, 而且包含 n 阶单位根群 G, 因而 $n|p^r-1$. 根据指数定义 $e\le r$. 另一方面, 由于 $n|p^e-1$, p^e-1 阶乘法群 $GF(p^e)^*$ 因为是循环的, 它包含一个 n 阶循环群即 n 次单位根群 G, 因而 $GF(p^e)$ 包含 E. 比较域的基数可知 $r\le e$. 所以 $r=e$. 设 $g(x)=x^r+a_1x^{r-1}+\cdots+a_r$ 为 ζ 的极小多项式, $a_i\in\mathbf{F}_p$. 将弗罗贝尼乌斯自同构 σ 作用于 $g(\zeta)$ 得 $\sigma(\zeta)^r+a_1\sigma(\zeta)^{r-1}+\cdots+a_r=\zeta^{pr}+a_1\zeta^{p(r-1)}+\cdots+a_r=0$,(这里 $\sigma(a_i)=a_i$) 即 $g(\zeta^p)=0$. 同理, $\zeta,\zeta^p,\cdots,\zeta^{p^{r-1}}$ 是 $g(x)$ 的全部根.

2) $\chi(P)=0$. 此时 $P=\mathbf{Q}$. 设 $f(x)$ 为 ζ 的极小多项式. 于是 $[E:\mathbf{Q}]=\deg f(x)$. 求证 $\deg f(x)=\varphi(n)$. 由于 $f(x)|x^n-1$ 但 $f(x)\nmid x^d-1, d<n$. 因而 $f(x)$ 与 x^d-1 互素, 所以 $f(x)$ 的根只能是本原 n 次单位根. 其次证明每个本原 n 次单位根都是 $f(x)$ 的根. 为此先证明一个基本事实: 对于 $f(x)$ 的任一根 ζ 和任一与 n 互素的素数 p, ζ^p 也是 $f(x)$ 的一根. 反证法, 假设 ζ^p 不是 $f(x)$ 的根. ζ^p 的极小多项式记作 $g(x)$. 则 $f(x)$ 与 $g(x)$ 互素, 从 $f(x)|x^n-1, g(x)|x^n-1$ 有 $f(x)g(x)|x^n-1$. x^n-1 可写成 $x^n-1=f(x)g(x)h(x)$, 注意 $f(x)$ 与 $g(x)$ 的首项系数为 1, 根据高斯引理, $f(x), g(x), h(x)$ 都是整系数多项式. 另一方面, $g(x)$ 以 ζ^p 为根, 则 $g(x^p)$ 以 ζ 为根. 从而 $f(x)|g(x^p)$ 而有 $g(x^p)=f(x)\cdot q(x)$, $q(x)$ 也是整系数多项式. 在自然同态 $\mathbf{Z}[x]\to\mathbf{Z}/(p)[x]$ 下, $f(x),\cdots$ 的象记作 $\overline{f}(x),\cdots$. x^n-1 的象仍记作 x^n-1.(注意前者 $x^n-1\in\mathbf{Z}[x]$, 后者 $x^n-1\in\mathbf{Z}/(p)[x]$.) 于是有

$$x^n-1=\overline{f}(x)\overline{g}(x)\overline{h}(x). \tag{1}$$

$$\overline{g}(x^p)=\overline{f}(x)\overline{q}(x). \tag{2}$$

将 $g(x)$ 明确写出 $g(x)=x^r+b_1x^{r-1}+\cdots+b_r$, $b_i\in\mathbf{Z}$. 于是 $\overline{g}(x^p)=x^{rp}+\overline{b}_1x^{(r-1)p}+\cdots+\overline{b}_r$, $\overline{b}_i\in\mathbf{F}_p$. 注意 $\chi(\mathbf{F}_p)=p$, 所以 $a^p=a, a\in\mathbf{F}_p$, 利用 $(a\pm b)^p=a^p\pm b^p$, 于是有 $\overline{g}(x^p)=(x^r+\overline{b}_1x^{r-1}+\cdots+\overline{b}_r)^p=\overline{g}(x)^p$. 因而 (2) 变成

$$\overline{g}(x)^p=\overline{f}(x)\overline{q}(x). \tag{3}$$

由于 $(p,n)=1$, x^n-1 在它的分裂域 $E/\mathbf{F}_p$ 内无重根, 从 (1) 式可知 $\overline{f}(x)$ 与 $\overline{g}(x)$ 互素. 但是由 (3) 式可知, $\overline{f}(x)$ 整除 $\overline{g}(x)^p$, 而且 $\deg\overline{f}(x)>0$, 因而 $\overline{f}(x)$ 不能与 $\overline{g}(x)$ 互素. 这是一个矛盾. 所以 ζ^p 必须是 $f(x)$ 的一根. 利用这个基本事实可证任一本原 n 次单位根 ζ 都是 $f(x)$ 的根. 因为 ζ 可以表成 $\zeta=\zeta^\nu, (\nu,n)=1$, 将 ν 分解成素因子的积 $\nu=p_1p_2\cdots p_r$ 而且 $(p_i,n)=1$. 令

$\zeta_0=\zeta,\zeta_1=\zeta^{p_1},\zeta_2=\zeta_1^{p_2},\cdots,\zeta_r=\zeta_{r-1}^{p_r}$. 于是 $\zeta=\zeta_r$. 根据基本事实可知，若 ζ_i 为 $f(x)$ 的一根，则 ζ_{i+1} 也是 $f(x)$ 的一根. 现在 $\zeta_0=\zeta$ 为 $f(x)$ 的一根. 从而推出 $\zeta_r=\zeta$ 也是 $f(x)$ 的一根. 这就证明了 $f(x)$ 的全部根恰好是全部本原 n 次单位根. 特别，$\deg f(x)=\varphi(n)$.

综上所述得到

定理 13 设 P 为一个素域，n 为一正整数. 当 $\chi(P)=$ 素数 p 时假定 $(n,p)=1$. 又设 E 为 x^n-1 在 P 上的分裂域. 则 E/P 是一个单扩张，可由任一本原 n 次单位根 ζ 生成 $E=P(\zeta)$. 而且

1) 若 $\chi(p)=$ 素数 p, 则 $[E:\mathbf{F}_p]=r$, 其中 r 为 $p \bmod n$ 的指数. 而且 ζ 的极小多项式 $f(x)=(x-\zeta)(x-\zeta^p)\cdots(x-\zeta^{p^{r-1}})$.

2) 若 $\chi(p)=0$, 则 $[E:\mathbf{Q}]=\varphi(n)$, 其中 $\varphi(n)$ 为欧拉函数，而且 ζ 的极小多项式 $\Phi(x)=\prod\limits_{\substack{1\le\nu<n\\(\nu,n)=1}}(x-\zeta^\nu)$. $\Phi(x)$ 叫做**分圆多项式**, $E=\mathbf{Q}(\zeta)$ 叫做 n **次分圆域**. □

根据定理 13,2) 我们可以做出 x^n-1 在 $\mathbf{Q}$ 上的分解式. 对 n 的每个因子 d, 有一个分圆多项式 $\Phi_d(x)$, 它的全部根恰好是全部本原 d 次单位根. 根据定理 13,2), $\Phi_d(x)$ 是一个 $\varphi(d)$ 次整系数不可约多项式而且 $\Phi_d(x)|x^n-1$. $\Phi_1(x)=x-1$. 对于 n 的不同因子 d_1,d_2, $\Phi_{d_1}(x)$ 与 $\Phi_{d_2}(x)$ 互素. 反之，x^n-1 的每个根必是某个 $\Phi_d(x)$ 的根. 因此得到 x^n-1 的分解式

$$x^n-1=\prod_{d|n}\Phi_d(x).$$

比较上式两边的次数，我们重新得到在第零章 §5 中得到过的公式

$$n=\sum_{d|n}\varphi(d).$$

分圆多项式也可以用 x^d-1 表示出来. 这需要用到默比乌斯函数 $\mu(n)$. $\mu(n)$ 是定义在正整数上的函数，其定义如下

$$\mu(n)=\begin{cases}1, & \text{当}n=1,\\ (-1)^r, & \text{当}n=p_1p_2\cdots p_r,\ p_i\text{为素数},p_i\ne p_j,i\ne j,\\ 0, & \text{当 } n \text{ 含素数平方因子}.\end{cases}$$

$\mu(n)$ 有一条很重要的性质

$$\sum_{d|n}\mu(d)=\begin{cases}1, & \text{当 } n=1,\\ 0, & \text{当 } n>1.\end{cases}$$

证明 当 $n=1$ 时，显然. 设 $n>1$ 而且 $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ 为素因子标准分解式，$e_i\geq 1$. 根据 $\mu(n)$ 的定义，不难看出

$$\sum_{d|n}\mu(d)=\sum_{d|n'}\mu(d),\quad n'=p_1p_2\cdots p_r.$$

而且

$$\begin{aligned}\sum_{d|n'}\mu(d)&=1+\sum_{1\leq\nu_1<\cdots<\nu_s\leq r}\mu(p_{\nu_1})\mu(p_{\nu_2})\cdots\mu(p_{\nu_s})\\&=\prod_{i=1}^{r}(1+\mu(p_i))=0.\quad\square\end{aligned}$$

最后我们证明

$$\Phi_n(x)=\prod_{d|n}(x^d-1)^{\mu(\frac{n}{d})}.$$

证明 注意上式右端分子、分母的根只能是 n 次单位根. 设 ζ 为任一 n 次单位根. 只要数一数因式 $x-\zeta$ 在右端出现的次数. ζ 的阶设为 d_1, 则 $d_1|n$. $x-\zeta|x^d-1$ 当而且仅当 $d_1|d$. 当 $d_1|d$ 时，若 $\mu\left(\frac{n}{d}\right)=1$, 则 $x-\zeta$ 在分子上出现一次. 若 $\mu\left(\frac{n}{d}\right)=-1$ 时，$x-\zeta$ 在分母上出现一次，因此，$x-\zeta$ 在右端出现的次数应为

$$\sum_{d_1|d|n}\mu\left(\frac{n}{d}\right).$$

它等于

$$\sum_{\frac{d}{d_1}|\frac{n}{d_1}}\mu\left(\frac{n/d_1}{d/d_1}\right)=\begin{cases}0, & d_1<n,\\ 1, & d_1=n.\end{cases}$$

因此当 $d_1<n$ 时 $(x-\zeta)$ 在右端不出现，当 $d_1=n$ 时，$x-\zeta$ 恰出现一次，这就证明了上述公式. $\square$

例 1 $\Phi_{12}(x)=(x^{12}-1)(x^6-1)^{-1}(x^4-1)^{-1}(x^2-1)=(x^6+1)(x^2+1)^{-1}=x^4-x^2+1$.

例 2 q 为一素数.

$$\begin{aligned}&\Phi_q(x)=(x^q-1)(x-1)^{-1}=x^{q-1}+x^{q-2}+\cdots+1,\\&\Phi_{q^r}(x)=(x^{q^r}-1)(x^{q^{r-1}}-1)^{-1}=x^{(q-1)q^{r-1}}+x^{(q-2)q^{r-1}}+\cdots+x^{q^{r-1}}+1.\end{aligned}$$

§7 完全域

基域 F 应具备什么条件能使得 F 上每个不可约多项式都是可分的？

定义 5 一个域 F 称为 **完全域**, 若 $F[x]$ 中每个不可约多项式都是可分的.

特征 0 的域是完全的.

§4 中的例子 $\mathbf{F}_p = \mathbf{Z}/(p), F = \mathbf{F}_p(t)$ 不是完全的.

定理 14 一个特征 p(素数) 的域 F 是完全的充要条件是 F 的每个元素在 F 内可开 p 次方, 即 $F^p = F$, 其中 $F^p = \{a^p \mid a \in F\}$.

证明 若 $F^p \neq F$, 则存在一个元素 $a \in F$ 但是 $a \notin F^p$, 即 a 在 F 内不能开 p 次方, 根据 §4 引理 2, $x^p - a$ 在 F 上不可约, 但是 $x^p - a$ 不可分, 所以 F 不完全. 设 $F^p = F$, 求证 $F[x]$ 中每个不可约多项式都是可分的. 反证法, 假若 $F[x]$ 中有一个不可分的不可约多项式 $f(x)$, 因为它不可分, 根据 §4 的讨论, $f(x)$ 可写成

$$f(x) = g(x^p),$$

其中 $g(x) = x^m + b_1x^{m-1} + \cdots + b_m \in F[x]$, 但是因为 $F^p = F$, b_i 在 F 内可开 p 次方, 即 $b_i = c_i^p$, $c_i \in F$, 令 $h(x) = x^m + c_1x^{m-1} + \cdots + c_m$, 将有

$$f(x) = h(x)^p,$$

$f(x)$ 将在 $F[x]$ 中是可约的, 矛盾. □

推论 1 有限域是完全的.

证明 设 F 为一特征 $p > 0$ 的有限域. 根据 §5, F 有一个弗罗贝尼乌斯自同构 σ, 它将元素 a 映到 a^p, 由于 σ 是满射, 有 $F^p = F$. 所以 F 是完全域. □

推论 2 完全域上的代数扩张还是完全的.

证明 设 F 为一个完全域, K/F 为一代数扩张, 若 F 的特征为 0, 则 K 当然是完全的, 因此不妨设 $\chi(F) = p > 0$. 对任一 $\alpha \in K$, 考虑中间域 $E = F(\alpha)$, E 有一个自同态 $\sigma : x \mapsto x^p$, 在这个自同态下, $\sigma(E) = \sigma(F)(\sigma(\alpha))$ 而且 $\sigma(\alpha)$ 在 $\sigma(F)$ 上的次数等于 α 在 F 上的次数, 由于 F 完全, $F^p = F$, 于是 $E^p = F(\alpha^p)$, $[E^p : F] = [E : F]$, 所以 $E^p = E$, 于是 $K^p = K$, 因而 K 完全. □

§8　本原元素

我们考虑这样一个问题, 即一个有限扩张 K/F 在什么条件下是单扩张.

设 K/F 为一个有限扩张, 如果 K 可以添加一个元素 α 到 F 上而得到 $K = F(\alpha)$, 则 α 叫做 K/F 的一个 **本原元素**. 因此, 一个有限扩张 E/F 是否是单扩张, 就看它有没有本原元素.

首先看有限域上的有限扩张. 设 F 为一个有限域, 含 q 个元素, K/F 为 n 次扩张, $\alpha_1, \cdots, \alpha_n$ 为它的一基, 于是 K 的每个元素 α 可以唯一地表成

$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$, $a_i \in F$, 由此可知, K 包含 q^n 个元素, 因此 K 也是一个有限域. K 的非零元素组成的乘法群 K^* 是一个有限交换群, 根据第三章 §7 定理 19, K^* 是一个循环群, 设 α 为 K^* 的一个生成元. 显然有 $K = F(\alpha)$, 因而 α 为 K/F 的一个本原元素. 但是 K/F 的一个本原元素不一定是 K^* 的生成元. 于是得

有限域上的有限扩张都是单扩张.

定理 15 设 K/F 为一个有限扩张, 如果将 K 写成 $K = F(\alpha_1, \cdots, \alpha_r)$ 使得 $\alpha_2, \cdots, \alpha_r$ 是可分元, 则 K/F 是单扩张.

证明 根据上面的讨论, 不妨设 F 为无限域. 对 r 作归纳法, 先证 $r = 2$ 的情况, 设 $K = F(\alpha, \beta)$, β 为可分元, 求证 K/F 为单扩张. 设 $f(x), g(x)$ 分别为 α 和 β 的极小多项式, 并设 E/K 为 $f(x)g(x)$ 在 K 上的分裂域, $\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_r$ 和 $\beta = \beta_1, \beta_2, \cdots, \beta_s$ 分别为 $f(x)$ 和 $g(x)$ 在 E 内的全部根, 考虑下列方程

$$\alpha_i + y\beta_j = \alpha_k + y\beta_1, \quad j \neq 1.$$

因为 $\beta_j \neq \beta_1, j \neq 1$, 每个方程在 F 内只有一个解, 方程个数有限而 F 的元素无限, 因而存在一个 $c \in F$ 使得

$$\alpha_i + c\beta_j \neq \alpha_k + c\beta_1,$$

对所有的 i, k, j, 只要 $j \neq 1$. 令 $\theta = \alpha_1 + c\beta_1$, 则 $f(\theta - cx)$ 和 $g(x)$ 仅有公共根 β_1, 因为 $x - \beta_1$ 是 $g(x)$ 的单因式, 所以 $f(\theta - cx)$ 和 $g(x)$ 的最大公因式为 $x - \beta_1$, 注意 $f(\theta - cx)$ 和 $g(x)$ 的系数都属于 $F(\theta)$, 在 $F(\theta)[x]$ 内存在两个多项式 $u(x)$ 和 $v(x)$ 使得 $u(x)f(\theta - cx) + v(x)g(x) = x - \beta_1$, 因而 $\beta_1 \in F(\theta)$, 跟着 $\alpha_1 = \theta - c\beta_1 \in F(\theta)$, 所以 $F(\alpha, \beta) \subset F(\theta)$. 反之显然 $F(\theta) \subset F(\alpha, \beta)$, 因而 $F(\alpha, \beta) = F(\theta)$. 其次, 将 K 写成 $F(\alpha_1, \alpha_2, \cdots, \alpha_r)$, $\alpha_2, \cdots, \alpha_r$ 为可分元, 于是 $K = F(\alpha_1, \alpha_2, \cdots, \alpha_r) = F(\alpha_1, \cdots, \alpha_{r-1})(\alpha_r)$, 对 r 作归纳法. 根据归纳法假设, $F(\alpha_1, \cdots, \alpha_{r-1})$ 可写成 $F(\alpha)$, 于是 $K = F(\alpha, \alpha_r)$, 再根据上面的证明, $F(\alpha, \alpha_r)$ 又可写成 $F(\theta)$, 于是 $K = F(\theta)$. □

推论 有限可分扩张 K/F 含有本原元素, 因而是一个单扩张.

证明 显然. □

§9 迹与范数

迹与范数是域论和代数中经常遇到的概念. 有许多重要性质可以通过迹与范数反映出来.

设 K/F 为域 F 上任一有限扩张. K 可看作 F 上有限维线性空间, 利用域的乘法可以得到域 K 的一个矩阵表示. 取定 K/F 的一基 $u_1,\cdots,u_n$. K 的每个元素 α 在 K 上引起一个线性变换 $\alpha_r: x\mapsto \alpha\cdot x, x\in K$. α_r 在基 $u_1,\cdots,u_n$ 下的矩阵记作 $A=(a_{ij})$, 则有

$$\alpha_r(u_1,\cdots,u_n)=(\alpha u_1,\cdots,\alpha u_n)=(u_1,\cdots,u_n)A.$$

用 λ 表示 F 上的一个未定元, E 表示 $n\times n$ 的单位矩阵, 则 $\lambda E-A$ 叫做 α(在基 u_i 下) 的特征矩阵, 行列式 $F(\lambda)=|\lambda E-A|$ 叫做 α 的特征多项式, $(a_{11}+a_{22}+\cdots+a_{nn})$ 和 $|A|$ 分别叫做 α 的 **迹** 和 **范数**. 记成

$$T_F^K(\alpha)=(a_{11}+a_{22}+\cdots+a_{nn}),$$
$$N_F^K(\alpha)=|A|.$$

将 $F(\lambda)$ 写出 $F(\lambda)=\lambda^n+a_1\lambda^{n-1}+\cdots+a_n$, 则

$$T_F^K(\alpha)=-a_1,\quad N_F^K(\alpha)=(-1)^n a_n,$$

根据线性代数的知识, α 的特征多项式是不依赖于基的选取的, 因而 α 的迹和范数也就不依赖于基的选取. 而且在同一基下若元素 α 和 β $(\in K)$ 所对应的矩阵分别为 A 和 B, 则 $a\alpha+b\beta$ $(a,b\in F)$ 和 $\alpha\cdot\beta$ 所对应的矩阵分别为 $aA+bB$ 和 $A\cdot B$. 因此我们得到迹和范数的基本性质如下:

1) $T_F^K(a\alpha+b\beta)=aT_F^K(\alpha)+bT_F^K(\beta),\quad a,b\in F$;

2) $N_F^K(\alpha\beta)=N_F^K(\alpha)\cdot N_F^K(\beta)$;

3) $N_F^K(a\alpha)=a^nN_F^K(\alpha),\quad a\in F^*$.

显然 $T_F^K(0)=0, N_F^K(1)=1$.

定理 16 *T_F^K 是 K 作为 F 上线性空间到 F 的线性映射. 特别 T_F^K 是加法群 K 到加法群 F 的同态. 它或者是一个满同态, 或者是一个零同态. N_F^K 是乘法群 K^* 到乘法群 F^* 的一个同态.*

证明 由性质 1) 可知 T_F^K 是一个线性映射, 只须指出, 若 T_F^K 不是零同态, 则它是满同态. 因为存在一个 $\alpha\in K$ 使得 $T_F^K(\alpha)=a\neq 0$. 于是对任意 $x\in F$ 有 $T_F^K(x\alpha)=xT_F^K(\alpha)=xa$.$F$ 在 T_F^K 下的象集为 $F\cdot a=F$. 由 2) 可知 N_F^K 是 K^* 到 F^* 的群同态. □

注 决定 K 在 N_F^K 下的象是一个重要而复杂的问题. 以后还有机会讨论这个问题.

下面的方法告诉我们, 计算一个元素 α 的迹与范数不必在 K/F 内去计算, 只要在 $F(\alpha)/F$ 内计算就够了. 利用迹与范数和基的选取无关这一优点, 我们

取定 K 对 $F(\alpha)$ 的一基 $v_1,\cdots,v_r$, 又取定 $F(\alpha)$ 对 F 的一基 $w_1,\cdots,w_s$. 于是 v_iw_j 就构成 K 对 F 的一基. 令

$$\alpha w_j=\sum_{k=1}^{s}a_{kj}w_k,\quad j=1,\cdots,s. \tag{1}$$

$A_1=(a_{kj})$, 于是在 $F(\alpha)/F$ 的基 w_j 下, α 所对应的矩阵为 A_1 因而

$$T_F^{F_1}(\alpha)=\sum_{i=1}^{s}a_{ii},\quad N_F^{F_1}(\alpha)=|A_1|,$$

其中 $F_1=F(\alpha)$. 将 v_i 乘 (1) 式得

$$\alpha w_jv_i=\sum a_{kj}w_kv_i,\quad j=1,\cdots,s, i=1,\cdots,r.$$

于是在 K/F 的基 $w_1v_1,\cdots,w_sv_1,w_1v_2,\cdots,w_sv_2,\cdots,w_1v_r,\cdots,w_sv_r$ 下 α 所对应的矩阵为准对角形

$$A=\begin{pmatrix}A_1 & & & 0\\ & A_1 & & \\ & & \ddots & \\ 0 & & & A_1\end{pmatrix}.$$

由此得到下列公式

$$\begin{aligned}T_F^K(\alpha)&=r\cdot T_F^{F_1}(\alpha),\\ N_F^K(\alpha)&=N_F^{F_1}(\alpha)^r,\end{aligned}\quad r=[K:F_1], F_1=F(\alpha). \tag{2}$$

令 $F_1(\lambda)=|\lambda E_s-A_1|$, 其中 E_s 为 $s\times s$ 单位矩阵, 则 $F_1(\lambda)$ 为 α 作为 F_1/F 的元素的特征多项式. 而 $F(\lambda)=|\lambda E-A|$ 是 α 作为 K/F 的元素的特征多项式, 它们的关系为

$$F(\lambda)=F_1(\lambda)^r,\ r=[K:F_1]. \tag{3}$$

根据上面的讨论, 在任意有限扩张中迹与范数的计算归结为在单代数扩张中本原元素的迹与范数的计算.

引理 1 设 K/F 是一个单代数扩张 $K=F(\theta)$, $f(x)$ 为它的极小多项式, 并设在它的分裂域 E/F 内 $f(x)=(x-\theta_1)(x-\theta_2)\cdots(x-\theta_n)$. 又设 σ_i 为 K 到 E 的 n 个 F- 嵌入使得 $\sigma_i(\theta)=\theta_i$.(这里, 若 θ_i 为 r 重根, 则 σ_i 重复 r 次. 因此 $\sigma_1,\cdots,\sigma_n$ 可能有相同的) 于是

$$\begin{aligned}T_F^K(\alpha)&=\sigma_1(\alpha)+\sigma_2(\alpha)+\cdots+\sigma_n(\alpha),\\ N_F^K(\alpha)&=\sigma_1(\alpha)\sigma_2(\alpha)\cdots\sigma_n(\alpha).\end{aligned}\quad \alpha\in K. \tag{4}$$

证明 首先证明当 $\alpha=\theta$ 时引理成立.

令 $f(x)=x^n+a_1x^{n-1}+\cdots+a_n$. θ 在 K/F 的基 $1,\theta,\cdots,\theta^{n-1}$ 下对应的矩阵为

$$A=\begin{pmatrix} 0 & & & & -a_n \\ 1 & 0 & & & \vdots \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -a_2 \\ & & & 1 & -a_1 \end{pmatrix},$$

由计算 θ 的特征多项式 $F(\lambda)=|\lambda I-A|=f(\lambda)=\lambda^n+a_1\lambda^{n-1}+\cdots+a_n$. 于是得 $T_F^K(\theta)=-a_1, N_F^K(\theta)=(-1)^na_n$ 即得 (4). 其次设 $\alpha\in K$ 为任意元素. 令 $F_1=F(\alpha)$, $f_1(x)$ 为 α 的极小多项式, 并在 E 内分解成 $f_1(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_s)$, $r=\dfrac{n}{s}$. 设 τ_i 为 F_1 到 E 内的 F- 嵌入使得 $\tau_i(\alpha)=\alpha_i$. 于是, 根据上面的讨论有

$$T_F^{F_1}(\alpha)=\tau_1(\alpha)+\cdots+\tau_s(\alpha),$$
$$N_F^{F_1}(\alpha)=\tau_1(\alpha)\cdots\tau_s(\alpha).$$

根据 (2), 得

$$\begin{aligned} T_F^K(\alpha)&=r(\tau_1(\alpha)+\cdots+\tau_s(\alpha)),\\ N_F^K(\alpha)&=(\tau_1(\alpha)\cdots\tau_s(\alpha))^r. \end{aligned} \tag{5}$$

另一方面, 每个 σ_i 是某个 τ_j 在 K 上的开拓, 因而 $\sigma_i(\alpha)$ 是 $f_1(x)$ 的根. 令 $g(x)=\prod_{i=1}^{n}(x-\sigma_i(\alpha))$. 则 $g(x)\in F[x]$ 而且 $g(x)$ 的每个根都是不可约多项式 $f_1(x)$ 的根, $g(x)$ 只能是 $f_1(x)$ 的一个方幂, 比较次数得 $g(x)=f_1(x)^r$. 由此可知

$$\sum_{i=1}^{n}\sigma_i(\alpha)=r\sum_{i=1}^{s}\tau_i(\alpha),$$
$$\prod_{i=1}^{n}\sigma_i(\alpha)=\prod_{i=1}^{s}\tau_i(\alpha)^r.$$

与 (5) 联系起来即得 (4). 于是引理一般成立. □

引理 2 *设 K/F 为单代数扩张, θ 为任一本原元素, $K=F(\theta)$. 则*

1) *若 K/F 不可分, 则 $T_F^K(\theta)=0$.*

2) *若 K/F 可分, 则 $T_F^K(\theta^i)$, $i=0,1,2,\cdots$ 不全为 0.*

证明 设 $f(x)$ 为 θ 的极小多项式, 在分裂域 E 中 $f(x)=(x-\theta_1)\cdots(x-\theta_n)$. σ_i 为 K 到 E 中的 F- 嵌入使得 $\sigma_i(\theta)=\theta_i$.

1) 设 K/F 不可分，则 F 的特征为一素数 p, 而且 θ 在 F 上不可分．于是 $f(x)$ 可写成 $f(x)=g(x^{p^e})$, 其中 $g(x)\in F[x]$ 为一 r 次不可约多项式．因此 $f(x)$ 只有 r 个不同的根，记为 $\theta_1',\cdots,\theta_r'$, 每个 θ_i' 是一个 p^e 重根．根据引理 1, 有

$$\begin{aligned}T_F^K(\theta)&=\sigma_1(\theta)+\cdots+\sigma_n(\theta)=\theta_1+\theta_2+\cdots+\theta_n\\&=p^e(\theta_1'+\cdots+\theta_r')=0.\end{aligned}$$

2) 设 K/F 可分，则 $f(x)$ 可分，它的根 $\theta_1,\cdots,\theta_n$ 两两不同．此时

$$\begin{aligned}T_F^K(\theta^i)&=\sigma_1(\theta^i)+\cdots+\sigma_n(\theta^i)\\&=\sigma_1(\theta)^i+\cdots+\sigma_n(\theta)^i\\&=\theta_1^i+\cdots+\theta_n^i,\qquad i=0,1,2,\cdots\end{aligned}$$

反证法．假如 $T_F^K(\theta^i),i=0,1,2,\cdots$ 全为 0, 于是将有

$$\theta_1^i+\theta_2^i+\cdots+\theta_n^i=0,\ \ i=0,1,\cdots,n-1.$$

从而推出范德蒙行列式 $|\theta_j^i|=0$. 但是 $\theta_1,\cdots,\theta_n$ 两两不等，这是一个矛盾．所以 $T_F^K(\theta^i)$, $i=0,1,\cdots,n-1$ 不能全为 0. □

定理 17 *设 K/F 为一个有限扩张．迹映射 $T_F^K:K\to F$ 是一个满同态当而且仅当 K/F 是可分扩张．*

证明 设 K/F 可分，则根据定理 15 的推论，K/F 是一个单扩张．$K=F(\theta)$. 根据引理 2, $T_F^K(\theta^i)$, $i=0,1,2,\cdots$ 不全为 0. 因而 T_F^K 不是零同态．再根据定理 16, T_F^K 是一个满同态．反之，设 K/F 为一个不可分扩张．求证 T_F^K 是一个零同态．设 $[K:F]=n$, 由于 K/F 不可分，$\chi(F)$ 为一素数 p 而且显然 $p|[K:F]$. 因而对于 F 的每个元素 a, 有 $T_F^K(a)=n\cdot a=0$. 设 α 为 K 的任一元素但 $\alpha\notin F$. 令 $F_1=F(\alpha)$. 则 $[F_1:F]>1$, $[K:F_1]<n$. 此时可应用公式 (2),

$$T_F^K(\alpha)=r\cdot T_F^{F_1}(\alpha),\ \ r=[K:F_1].$$

由于 K/F 不可分，根据定理 10, F_1/F 和 K/F_1 两者中必有一个是不可分扩张．若 F_1/F 不可分，则根据引理 2, $T_F^{F_1}(\alpha)=0$, 因而 $T_F^K(\alpha)=0$, 若 K/F_1 不可分，则 $p|r$. 因而也有 $T_F^K(\alpha)=0$. 总之 $T_F^K(\alpha)=0$. 于是对 K 的所有元素 α, $T_F^K(\alpha)=0$. 所以 T_F^K 是一个零同态． □

习 题

1. 设 K/F 为一个有限域扩张，且 $[K:F]=p$ 为一素数．证明：任一元素 $\alpha\in K\setminus F$ 在 F 上生成 K, 即 $K=f(\alpha)$.

2. 设 K/F 为一有限扩张，$\alpha \in K$ 是 F 上一个 n 次元素，则 $n|[K:F]$.

3. 设 L, M 为域 K 的两个子域. K 中包含 L 和 M 的一切子域的交叫做子域 L 和 M 在 K 中的复合域，记作 $L \cdot M$. 证明：

(i) 设 $L \cap M = F$, 若 L 和 M 分别由子集 S 和 T 在 F 上生成，即 $L = F(S), M = F(T)$, 则 $L \cdot M = F(S \cup T)$.

(ii) 若 L 由子集 S 在 F 上生成，则 $L \cdot M = M(S)$.

(iii) $L \cdot M \supseteq L \cup M$, 在什么条件下等号成立？

4. 设 K 为 F 上域扩张. 证明：如果 $u \in K$ 是 F 上代数元而且次数为奇数，则 u^2 也是 F 上奇次代数元而且 $F(u) = F(u^2)$.

5. 证明：若 $x^n - a \in F[x]$ 不可约，则对于任一正整数 $m|n, x^m - a$ 在 F 上也不可约.

6. 求下列扩域的一基：

(i) $K = \mathbf{Q}(\sqrt{2}, \sqrt{3})$;

(ii) $K = \mathbf{Q}(\sqrt{3}, \sqrt{-1}, \omega)$, 其中 $\omega = \dfrac{1}{2}(-1 + \sqrt{-3})$.

7. 在 $\mathbf{Q}(\sqrt{-1})$ 和 $\mathbf{Q}(\sqrt{2})$ 之间不存在 $\mathbf{Q}$- 同构.

8. 设 L 和 M 为域扩张 K/F 的中间域. 证明：

(i) $[LM:F]$ 有限当而且仅当 $[L:F]$ 和 $[M:F]$ 都有限；

(ii) $[LM:F] \leq [L:F] \cdot [M:F]$;

(iii) 若 $[L:F]$ 与 $[M:F]$ 互素，则 (ii) 中等式成立；

(iv) 若 L/F 和 M/F 都是代数的，则 $L \cdot M/F$ 也是代数的.

9. 证明：若 K/F 是一个代数扩张，则 K 的任一个 F- 自同态 σ 是一个 F- 自同构.

10. 决定下列多项式在有理数域上的分裂域：

(i) $f(x) = x^4 - 2$;

(ii) $f(x) = x^3 - 2x - 2$;

(iii) $f(x) = x^3 - 3x - 1$.

11. 决定 $x^{p^e} - 1$. $e \geq 1$, 在特征 p 的素域 $\mathbf{F}_p = \mathbf{Z}/(p)$ 上的分裂域.

12. 决定 $x^6 + 2x^3 + 2$ 在 $\mathbf{F}_3 = \mathbf{Z}/(3)$ 上的分裂域.

13. 设 E 是多项式 $f(x) \in F[x]$ 在 F 上的分裂域，K 为 E/F 的一个中间域，证明 E 也是 $f(x)$ 在 K 上的分裂域.

14. 设 $F \subset K \subset L$ 是代数扩张链. 如果 L/K 和 K/F 都是正规的，问 L/F 是否是正规的？

15. 证明：若域扩张 E/F 的中间域 K 在 F 上正规，则 K 关于 E/F 是稳定的，即对于 E 的任一个 F- 自同构 σ 恒有 $\sigma(K) = K$.

16. 设 E/F 为有限正规，K 为它的中间域. 证明：K 在 F 上正规的充要条件是 K 关于 E/F 是稳定的.

17. 设 K, L 是域扩张 E/F 的两个中间域. 证明：如果 K/F 和 L/F 都正规，则复合域 $K \cdot L$ 和 $K \cap L$ 在 F 上都正规.

18. 设 K, L 是域扩张 E/F 的两个中间域. 证明：如果 K/F 正规，则 $K \cdot L$ 在 L 上也正规.

19. 设 E/F 为有限正规扩张，$f(x) \in F[x]$ 在 F 上不可约. 证明:

(i) $f(x)$ 在 E 上分解成次数相等的不可约多项式 $f_1(x), f_2(x), \cdots, f_r(x)$ 的同方幂的乘积，即

$$f(x) = [f_1(x)f_2(x)\cdots f_r(x)]^{p^e}, \ e \geq 0,$$

其中 $f_i(x)$ 为不相伴的不可约多项式，而且当 F 的特征为 0 时，$e = 0$, 当 F 的特征为素数 p 时，$e \geq 0$.(设 $f(x)$ 的首项系数为 1.)

(ii) 设 E 的全部 F- 自同构组成的群记作 G. 令 $H = \{\sigma \in G \mid f_1^{\sigma}(x) = f_1(x)\}$(当然取 $f_1(x)$ 的首项系数为 1). 于是，令 $G = \sigma_1 H \cup \sigma_2 H \cup \cdots \cup \sigma_{r'} H, \sigma_1 = 1$, 则有

$$f(x) = \left[\prod_{i=1}^{r'} f_1^{\sigma_i}(x)\right]^{p^e}.$$

从而 $r' = r$.

20. 设 E/F 为一个有限正规扩张，G 表示 E 的全部 F- 自同构组成的群. 证明:

(i) 令 $L = \{\alpha \in E \mid \sigma(\alpha) = \alpha 对所有 \sigma \in G\}$, 则 L 是 E 的子域，包含 F 而且 L 是 F 上的纯不可分扩张. L 叫做 G 的**不动域**.

(ii) 用 K 表示 F 在 E 内的可分闭包，则 K 在 F 上正规.

(iii) $E = L \cdot K, L \cap K = F$.

(iv) 用 G' 表示 K 的全部 F- 自同构组成的群，则

$$G' \cong G.$$

对每个 $\sigma \in G, \sigma$ 在 K 上诱导出 K 的一个 F- 自同构 σ'. 于是映射 $\sigma \mapsto \sigma'$ 给出 G 到 G' 的一个同构.

21. (i) 构造一个 9 个元素的域并给出加法和乘法表.

(ii) 构造一个 8 个元素的域并给出加法和乘法表.

22. 设 $\mathbf{F}_p = \mathbf{Z}/(p)$, p 为素数，$f(x) \in \mathbf{F}_p[x]$ 为一个 n $(n \geq 1)$ 次不可约多项式，$P_n(x)$ 表示 $\mathbf{F}_p[x]$ 中首项系数为 1 的 n 次不可约多项式全体的乘积. 证明:

(i) $f(x) | x^{p^m} - x$ 当而且仅当 $n | m$;

(ii) $x^{p^n} - x | x^{p^m} - x$ 当而且仅当 $n | m$;

(iii) $x^{p^n} - x = \prod_{d|n} P_d(x)$;

(iv) $P_n(x) = \prod_{d|n} (x^{p^d} - x)^{\mu(\frac{n}{d})}$,

其中 $\mu(n)$ 为默比乌斯函数;

(v) $\mathbf{F}_p$ 上 n 次不可约多项式 (互不相伴) 的个数等于

$$N_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

*23. 证明 $x^{2^n} + x + 1$ 在 $\mathbf{F}_2$ 上不可约.

24. 证明有限域的每个元素可表成两元素的平方和.

25. 证明：若 L/K 是纯不可分扩张而且 K/F 是纯不可分扩张，则 L/F 也是纯不可分扩张.

26. 设在一域扩张 K/F 中元素 α 和 β 分别是 F 上可分元素和纯不可分元素. 证明：

(i) $F(\alpha,\beta)=F(\alpha+\beta)$;

(ii) 当 $\alpha\neq 0,\beta\neq 0, F(\alpha,\beta)=F(\alpha\beta)$.

27. 设域 F 的特征为素数 p. 证明：若 $a\in F$ 但 $a\notin F^p$, 则 $x^{p^e}-a\ (e\geq 1)$ 在 F 上不可约.

28. 设域 F 的特征为素数 p, 证明：

(i) 若多项式 $f(x)\in F[x]$ 不可约而且 $f(x)$ 的次数与 p 互素，则 $f(x)$ 在 F 上可分.

(ii) 若有限扩张 K/F 的次数 $[K:F]$ 与 p 互素，则 K/F 是可分扩张.

29. 设域 F 的特征为素数 p, K 为 F 上扩域. 证明： K 的元素 α 在 F 上是代数的而且可分的充要条件是 $F(\alpha)=F(\alpha^{p^n})$ 对所有 $n\geq 1$ 都成立.

30. 证明：一个有限扩张 K/F 是纯不可分的充要条件是 K/F 到 K 的正规闭包 E/F 的 F- 嵌入只能是恒等嵌入.

31. 设 $\mathbf{F}_p[x,y]$ 是 $\mathbf{F}_p$ 上二元多项式环, $K=\mathbf{F}_p(x,y)$ 表示 $\mathbf{F}_p[x,y]$ 的商域. 令 $K^p=F$. 证明：

(i) $F=\mathbf{F}_p(x^p,y^p)$;

(ii) K 不是 F 上的单扩张;

(iii) 在 K 与 F 之间存在无穷多个中间域.

32. 利用 §6 的公式，证明分圆多项式 Φ_n 有性质：

(i) 设 $n=p_1^{r_1}\cdots p_s^{r_s}, p_i$ 为不同素数， $r_i\geq 1$, 则

$$\Phi_n(x)=\Phi_{p_1\cdots p_r}(x^{p_1 r_1-1\cdots p_s r_s-1}).$$

(ii) 设 n 为奇数，则

$$\Phi_{2n}(x)=\Phi_n(-x).$$

(iii) 设 p 为素数且 $p\nmid n$, 则

$$\Phi_{pn}(x)=\Phi_n(x^p)/\Phi_n(x).$$

33. 设 ζ 为复数域中一个本原 n 次单位根. 证明 $[\mathbf{Q}(\zeta+\zeta^{-1}):\mathbf{Q}]=\dfrac{1}{2}\varphi(n)$ (假定 $n>2$). 因而 $\mathbf{Q}(\zeta+\zeta^{-1})$ 是 $\mathbf{Q}(\zeta)$ 的最大实子域.

34. 设域 F 的特征为素数 $p, K/F$ 为一代数扩张. 证明：对于每个元素 $\alpha\in K$, 存在一个适当的方幂 α^{p^r} 使得 α^{p^r} 在 F 上可分. 当 $[K:F]=n<\infty$ 时，有 $r\leq\dfrac{\log n}{\log p}$.

35. 设域 F 的特征为素数 $p, K/F$ 为一个代数扩张. K^{p^r} 表示集合 $\{\alpha^{p^r}\mid\alpha\in K\}$. 证明：若 $[K:F]<\infty$, 则存在一个适当正整数 r 使得 $F(K^{p^r})$ 在 F 上可分而且是 F 在 K 中的可分闭包.

36. 设 K/F 为有限扩张. 证明：若 K/F 为单扩张，则域特征 $\chi(F)=0$ 或者 $\chi(F)=p>0$ 而且 $[K:F(K^p)]\leq p$.

37. 设 K/F 为有限扩张. 证明：若域特征 $\chi(F)=0$ 或者 $\chi(F)=p>0$ 而且 $[K:F(K^p)]\leq p$, 则 K/F 是单扩张.

38. 设 K/F 为一个代数单扩张. 令 $K=F(\theta)$. 又设 L 为 K/F 的任一个中间域. 证明： θ 在 L 上的极小多项式 $g(x)=x^r+\alpha_1x^{r-1}+\cdots+\alpha_r$ 的系数 $\alpha_1,\cdots,\alpha_r$ 在 F 上生成的子域 $F(\alpha_1,\cdots,\alpha_r)$ 就是 L. 并由此进一步证明，代数单扩张 K/F 只有有限多个中间域.

39. 设 F 为一个无限域， K/F 为一个代数扩张. 证明：若 K/F 只有有限多个中间域，则对于任意元素 $\alpha,\beta\in K$, $F(\alpha)$ 和 $F(\beta)$ 在 K 内的复合域仍然是 F 上的一个单扩张. 由此进一步证明，若代数扩张 K/F 只有有限多个中间域，则 K/F 是一个单扩张.

40. 证明单代数扩张 K/F 的中间域 L/F 仍是一个单扩张.

41. 设 $F=\mathbf{Q}(\sqrt{-1})$. 试决定 F 到 $\mathbf{Q}$ 的范数群 $N_{\mathbf{Q}}^F(F^*)=\{N_{\mathbf{Q}}^F(\alpha)\,|\,\alpha\in F^*\}$.(参看第四章习题 18.)

42. 设 $K=GF(p^n)$. 直接证明 K 到子域 $\mathbf{F}_p$ 的范数群 $N_{\mathbf{F}_p}^K(K^*)=\mathbf{F}_p^*$.

43. 证明复数域 $\mathbf{C}$ 到实数域 $\mathbf{R}$ 的范数群 $N_{\mathbf{R}}^{\mathbf{C}}(\mathbf{C}^*)=\mathbf{R}^+=\{\alpha\in\mathbf{R}\,|\,\alpha>0\}$.

第八章　伽罗瓦理论

引言　一个多项式的根如何用它的系数经过四则运算和开方表示出来即所谓用根式解方程的问题，是 19 世纪以前代数的一个主要问题. 大约在公元前 1700 年人们就已经知道一元二次方程的解法. 但是三、四次方程直到公元 1500 年左右才由费罗 (Férro) 、塔塔格利亚 (Tartaglia) 、卡尔塔诺(Cardano) 和费拉利 (Ferrari) 等人先后给出解的公式. 从此以后，人们致力于五次以上方程的代数解法，但经过近三百年的努力一直未能成功. 其间值得提出的有拉格朗日、鲁菲尼 (Ruffini) 和阿贝尔. 拉格朗日在他 1772 年发表的著作中，对二、三、四次一般方程的可解性作了透彻的分析，提出了 n 次一般方程 $f(x)$ 的预解式的概念，即量 $t = x_1 + \zeta x_2 + \cdots + \zeta^{n-1}x_n$, 其中 x_i 为 $f(x)$ 的根，ζ 为任一 n 次单位根. 如果能先解出 t, 然后就能解出 x_i. 这对二、三、四次一般方程是一个统一有效的方法. 但是对五次一般方程则遇到了不可克服的困难. 拉格朗日还证明两个关键性的定理. 一个根的置换 π 在根的有理函数 $\varphi(x_1, \cdots, x_n)$ 上的作用规定为 $\phi^\pi(x_1, \cdots, x_n) = \phi(\pi(x_1), \cdots, \pi(x_n))$. 定理 I 是说：如果凡是保持根的有理函数 ϕ 不变的根的置换也保持根的有理函数 ψ 不变，则 ψ 可以表成 ϕ 和 $f(x)$ 的系数的有理函数. 定理 II 是说：如果凡是保持 ϕ 不变的根的置换都保持 ψ 不变，而且保持 ψ 不变的根置换全体作用在 ϕ 上产生 r 个不同的值 $\phi_1, \cdots, \phi_r$, 则 $\phi_1, \cdots, \phi_r$ 同时一个 r 次多项式的根，其系数是 ψ 和 $f(x)$ 的系数的有理函数. 后来，鲁菲尼和阿贝尔先后独立地证明了五次以上一般方程的根是不能用根式解的. 另一方面，高斯在他 1801 年发表的经典著作中证明了，一个素数 p 次单位根 ζ 可用 $g(x) = x^p + x^{p-1} + \cdots + 1$ 的预解式

$$t_i = \zeta + \xi^i\zeta^g + \xi^{2i}\zeta^{g^2} + \cdots + \xi^{(p-2)i}\zeta^{g^{p-2}}, \quad i = 1, 2, \cdots, p-1$$

表示出来

$$\zeta = \frac{1}{p-1}(t_1 + t_2 + \cdots + t_{p-1}),$$

其中 ξ 为一个本原 $p-1$ 次单位根，g 为 $\mathrm{mod}\, p$ 的一个原根. 而且 $t_i^{p-1} = a_i$ 是 ξ 的有理函数. 由此可知，本原 p 次单位根可以用根式表示出来，其中出现的根指数都低于 p. 从而将 ζ 的根式解化为求解一串素数次的二项方程.

天才的伽罗瓦 (1811–1832) 悉心研究了拉格朗日、阿贝尔和高斯的著作之后，对任一个 n 次方程 $f(x)$(无重根，系数 $a_1, \cdots, a_n$ 是数值的或是未定元都可以) 给出了新的预解式概念，它是根的线性函数 $t = b_1x_1 + \cdots + b_nx_n$, 在根的置换下产生 $n!$ 个不同的值，其中 $b_1, \cdots, b_n \in F = \mathbf{Q}(a_1, \cdots, a_n)$. 设 $g(x) \in F[x]$ 为 t 所适合的不可约多项式. 伽罗瓦定义方程 $f(x)$ 的群 G_f 为使 $g(t^\pi) = 0$ 的

全部根的置换 π 所组成的集合. 由此伽罗瓦才有可能将 $f(x)$ 的根可用根式解的条件转化成它的群 G_f 所应具备的条件, 那就是 G_f 应是可解的. 这是伽罗瓦所取得的突出的成就. 在提出了方程的群之后, 伽罗瓦接着就证明了它的一条基本性质:

根的有理函数 $\phi(x_1,\cdots,x_n)$ 属于基域 F 当而且仅当在 G_f 的所有置换作用下 $\phi(x_1,\cdots,x_n)$ 的值保持不变.

这条性质表明, 根之间在 F 上的代数关系完全可以由方程的群所刻画.

我们将以此为出发点来建立伽罗瓦理论.

§1 伽罗瓦扩张、基本定理

定义 1 设 K/F 为任一域扩张. K 的全部 F- 自同构成一群, 叫做 K/F 的 **伽罗瓦群**, 记成 $\mathrm{Gal}(K/F)$.

说明 在定义 1 中的基域可以是特征 0 的域也可以是特征 $p>0$ 的域.

定义 2 设 G 为域 K 的任一个自同构群. 若 K 的元素 α 满足 $\sigma(\alpha)=\alpha$ 对所有 $\sigma\in G$, 则 α 叫做 G 的一个 **不动元**. K 中 G 的不动元全体记成 $\mathrm{Inv}(G)$. $\mathrm{Inv}(G)$ 形成 K 的一个子域, 叫做 G 的 **不动域**.

下面我们来证明 $\mathrm{Inv}(G)$ 确实为一子域.

对于任意元 $\alpha,\beta\in\mathrm{Inv}(G)$, 有

$$\sigma(\alpha-\beta)=\sigma(\alpha)-\sigma(\beta)=\alpha-\beta,$$
$$\sigma(\alpha/\beta)=\sigma(\alpha)/\sigma(\beta)=\alpha/\beta,\quad \beta\neq 0.$$

对所有 $\sigma\in G$ 都成立, 因而 $\alpha-\beta,\alpha/\beta\ (\beta\neq 0)$ 都属于 $\mathrm{Inv}(G)$. 特别 $0,1\in\mathrm{Inv}(G)$. 所以 $\mathrm{Inv}(G)$ 是 K 的一个子域.

任意域扩张 K/F 的伽罗瓦群 $\mathrm{Gal}(K/F)=G$ 的不动域 $\mathrm{Inv}(G)$ 包含 F 但可以大于 F. 设 G_1,G_2 为域 K 的两个自同构群. 若 $G_1\subset G_2$, 则显然有 $\mathrm{Inv}(G_1)\supset\mathrm{Inv}(G_2)$.

例 1 设 $F=\mathbf{Q}$ 有理数域, $K=\mathbf{Q}(\sqrt[3]{2})$. $\sqrt[3]{2}$ 表示 x^3-2 的一个实根. 显然 $\mathrm{Gal}(K/\mathbf{Q})=I$ 单位元群. 此时 $\mathrm{Inv}(I)=K$.

例 2 设 $F=\mathbf{F}_p(t)$ 为特征 p 的素域 $\mathbf{F}_p$ 上有理分式域. 令 $g(x)=x^2+tx+t, f(x)=g(x^p)$. 设 E/F 为 $f(x)$ 的分裂域. $f(x)$ 只有两个不同的根, 记为 α,β. 由于 $g(x)$ 在 F 上不可约, $f(x)$ 在 F 上也不可约. E 只有一个非平凡 F- 自同构 σ 将 α 变成 β. 因而 $\mathrm{Gal}(E/F)=\langle\sigma\rangle$ 是一个二阶群. 令 $\alpha+\beta=a,\alpha\cdot\beta=b,F_1=F(a,b)$. 易见 $a^p=-t,b^p=t$. 由此可知 $\mathrm{Gal}(E/F)$ 的不动域包含 F_1. 读者不难证明, F_1 就是 $\mathrm{Gal}(E/F)$ 的不动域.

从例 1 和例 2 看出，当域扩张 K/F 不正规或不可分时， $\mathrm{Gal}(E/F)$ 的不动域可以大于 F. 下面将会看到．在这些情况， $\mathrm{Gal}(E/F)$ 的不动域一定比 F 大.

定义 3 若域扩张 E/F 的 $\mathrm{Gal}(E/F)$ 的不动域等于 F, 则 E/F 叫做一个 **伽罗瓦扩张**, 或说 E 在 F 上是伽罗瓦的.

一般说来，设 F_1 为域扩张 E/F 的 $\mathrm{Gal}(E/F)$ 的不动域，则 E 是 F_1 上的伽罗瓦扩张.

这是现在流行的伽罗瓦扩张的定义．原来意义的伽罗瓦扩张是指以有理数域的一个扩域 F 为基域， F 上一个无重根的多项式 $f(x)$ 的分裂域．下面首要的任务是建立伽罗瓦理论的基本定理，然后证明这两种定义是等价的.

现在的定义是突出了伽罗瓦群的地位和作用，强调了它和基域的关系．但是从定义一点也看不出 E 对 F 的次数和伽罗瓦群 $\mathrm{Gal}(E/F)$ 的阶有什么关系．下面两个引理完全确定了这两者的关系.

引理 1 (**阿廷**(Artin)) 设 G 为域 K 的一个有限自同构群， F 为它的不动域，则 $[K:F]\le|G|$.

证明 设 $|G|=n, G=\{\sigma_1=1,\sigma_2,\cdots,\sigma_n\}$. 设 $u_1,u_2,\cdots,u_{n+1}$ 为 K 的任意 $n+1$ 个元素，全不为 0. 用 σ_i 作用于 u_j 得到一个 $n\times(n+1)$ 矩阵

$$\begin{pmatrix} \sigma_1(u_1) & \sigma_1(u_2) & \cdots & \sigma_1(u_{n+1}) \\ \sigma_2(u_1) & \sigma_2(u_2) & \cdots & \sigma_2(u_{n+1}) \\ \cdots & \cdots & \cdots & \cdots \\ \sigma_n(u_1) & \sigma_n(u_2) & \cdots & \sigma_n(u_{n+1}) \end{pmatrix},$$

列向量 $\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_{n+1}$ 显然在 K 上线性相关．于是存在一个整数 r, $1\le r<n+1$, 使得 $\boldsymbol{v}_1,\cdots,\boldsymbol{v}_r$ 线性无关而 $\boldsymbol{v}_1,\cdots,\boldsymbol{v}_{r+1}$ 则线性相关．从而 $\boldsymbol{v}_{r+1}$ 可以唯一地表成

$$\boldsymbol{v}_{r+1}=\alpha_1\boldsymbol{v}_1+\cdots+\alpha_r\boldsymbol{v}_r,\quad \alpha_i\in K. \tag{1}$$

用分量的形式写出就是

$$\sigma_i(u_{r+1})=\alpha_1\sigma_i(u_1)+\cdots+\alpha_r\sigma_i(u_r),\quad i=1,\cdots,n. \tag{2}$$

用 $\sigma\in G$ 作用于 (2) 得

$$\sigma\sigma_i(u_{r+1})=\sigma(\alpha_1)\sigma\sigma_i(u_1)+\cdots+\sigma(\alpha_r)\sigma\sigma_i(u_r),\ i=1,\cdots,n. \tag{3}$$

由于 G 是一群， $\sigma\sigma_1,\cdots,\sigma\sigma_n$ 不过是 $\sigma_1,\cdots,\sigma_n$ 的一个排列，所以，将 (3) 中等式的次序作适当调换，再恢复列向量的写法得

$$\boldsymbol{v}_{r+1}=\sigma(\alpha_1)\boldsymbol{v}_1+\cdots+\sigma(\alpha_r)\boldsymbol{v}_r,\quad 对所有\ \sigma\in G. \tag{4}$$

与 (1) 比较，由表法的唯一性得 $\sigma(\alpha_j)=\alpha_j$ 对所有 $\sigma\in G$ 和 $j=1,\cdots,r$，从而 $\alpha_j\in \mathrm{Inv}(G)$. 但 $\mathrm{Inv}(G)=F$，所以 $\alpha_j\in F$，$j=1,\cdots,r$. 由 (2) 的第一个等式 $u_{r+1}=\alpha_1u_1+\cdots+\alpha_ru_r$ 可知 $u_1,\cdots,u_{r+1}$ 在 F 上线性相关，当然 $u_1,\cdots,u_{n+1}$ 在 F 上也线性相关. 所以 $[K:F]\le|G|$ □

引理 2 *设 $\sigma_1,\cdots,\sigma_r$ 是域 K 到域 E 的 r 个不同的单一同态，则 $\sigma_1,\cdots,\sigma_r$ 在 E 上线性无关. 就是说，若存在一个线性组合 $f(x)=\alpha_1\sigma_1(x)+\cdots+\alpha_r\sigma_r(x)$，$\alpha_1,\cdots,\alpha_r\in E$，使得 $f(x)=0$ 对所有 $x\in K$，则 $\alpha_1=\cdots=\alpha_r=0$.*

证明 将 $\sigma_1(x),\cdots,\sigma_r(x)$ 看作定义在 K 上的函数，取值在 E 中. 反证法，假若 $\sigma_1(x),\cdots,\sigma_r(x)$ 在 E 上线性相关. 则存在一个整数 s，$1\le s<r$，使得 $\sigma_1(x),\cdots,\sigma_s(x)$ 在 E 上线性无关而 $\sigma_1(x),\cdots,\sigma_{s+1}(x)$ 线性相关. 于是 $\sigma_{s+1}(x)$ 可以唯一地表成

$$\sigma_{s+1}(x)=\alpha_1\sigma_1(x)+\cdots+\alpha_s\sigma_s(x),\quad \alpha_i\in E. \tag{5}$$

$\alpha_1,\cdots,\alpha_r$ 至少有一个不为 0，不妨设 $\alpha_1\ne 0$. 由于 $\sigma_{s+1}\ne\sigma_1$，存在一个元素 $a\in K$ 使得 $\sigma_{s+1}(a)\ne\sigma_1(a)$. (5) 中用 ax 替换 x 得

$$\begin{aligned}\sigma_{s+1}(a)\sigma_{s+1}(x)&=\alpha_1\sigma_1(a)\sigma_1(x)+\cdots+\alpha_s\sigma_s(a)\sigma_s(x),\\ \sigma_{s+1}(x)&=\frac{\alpha_1\sigma_1(a)}{\sigma_{s+1}(a)}\sigma_1(x)+\cdots+\frac{\alpha_s\sigma_s(a)}{\sigma_{s-1}(a)}\sigma_s(x).\end{aligned}$$

与 (5) 比较，$\sigma_1(x)$ 的系数不相等，这与表法的唯一性矛盾. 所以 $\sigma_1(x),\cdots,\sigma_r(x)$ 在 E 上线性无关. □

推论 *设 $\sigma_1,\cdots,\sigma_r$ 是域 E 的 r 个不同的自同构，F 为集合 $S=\{\sigma_1,\cdots,\sigma_r\}$ 的不动域，则 $|S|\le[E:F]$. (其中 S 的不动域理解为由 S 生成的群的不动域.)*

证明 不失一般性，假设次数 $[E:F]=n$ 有限. 由于每个 $\sigma\in S$ 保持 F 的元素不动，则 σ 是线性空间 E/F 的一个线性变换：对 $\alpha,\beta\in E,a\in F$，

$$\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta),\ \sigma(a\alpha)=\sigma(a)\sigma(\alpha)=a\sigma(\alpha).$$

于是 $\sigma_1,\cdots,\sigma_r$ 在 E 上的任一个线性组合

$$\alpha_1\sigma_1+\alpha_2\sigma_2+\cdots+\alpha_r\sigma_r,\quad \alpha_i\in E \tag{6}$$

仍为 E/F 的一个线性变换. 根据引理 2 可知，(6) 为零变换的充要条件是 α_i 全为零. 另一方面，我们知道，E/F 的一个线性变换为零的充要条件是它把 E/F 的一基 $u_1,\cdots,u_n$ 的每个 u_j 变成零. 联结这两者得 (6) 式中 α_i 全为零的充要条件是

$$(\alpha_1\sigma_1+\cdots+\alpha_r\sigma_r)(u_j)=0,\quad j=1,\cdots,n,$$

即 $\alpha_1\sigma_1(u_j)+\alpha_2\sigma_2(u_j)+\cdots+\alpha_r\sigma_r(u_j)=0,\ j=1,\cdots,n$. 这表明下列 r 个向量

$$(\sigma_i(u_1),\sigma_i(u_2),\cdots,\sigma_i(u_n)),\quad i=1,\cdots,r$$

在 E 上线性无关. 所以 $r\leq n$. □

这个推论本来已包含在第七章定理 9 中. 但是这里是从一个完全不同的角度 (引理 2) 得到的.

定理 1 1) *若 K/F 为有限伽罗瓦扩张, 则 $\mathrm{Gal}(K/F)$ 的阶等于次数 $[K:F]$.*

2) *若域 K 有一个有限自同构群 G 以 F 为不动域, 则 K/F 为有限伽罗瓦扩张而且 $G=\mathrm{Gal}(K/F)$.*

3) *若有限扩张 K/F 有一个 F- 自同构群 G, 使得 $|G|=[K:F]$, 则 K/F 为伽罗瓦扩张而且 $G=\mathrm{Gal}(K/F)$.*

证明

1) 由于 $\mathrm{Inv}(\mathrm{Gal}(K/F))=F$, 根据引理 2 的推论 $|\mathrm{Gal}(K/F)|\leq[K:F]$. 又根据引理 1, 有 $[K:F]\leq|\mathrm{Gal}(K/F)|$. 所以 $|\mathrm{Gal}(K/F)|=[K:F]$.

2) 一方面由定义有 $F\subset\mathrm{Inv}(\mathrm{Gal}(K/F))$. 另一方面, 由 $G\subset\mathrm{Gal}(K/F)$ 有 $\mathrm{Inv}(\mathrm{Gal}(K/F))\subset\mathrm{Inv}(G)=F$. 因而 $\mathrm{Inv}(\mathrm{Gal}(K/F))=F$, 从而 K/F 是一个伽罗瓦扩张. 其次将引理 1 和引理 2 的推论用于群 G, 得 $|G|=[K:F]$. 根据 1), $|G|=|\mathrm{Gal}(K/F)|$. 由 $G\subset\mathrm{Gal}(K/F)$ 即得 $G=\mathrm{Gal}(K/F)$.

3) 设 $\mathrm{Inv}(G)=F_1$. 求证 $F_1=F$. 根据 2) 可知 K 是 F_1 上伽罗瓦扩张而且 $G=\mathrm{Gal}(K/F_1)$. 再由 1) 得 $|G|=[K:F_1]$. 根据假设得 $[K:F_1]=[K:F]$. 注意 $F\subset F_1$, 从而得 $[F_1:F]=[K:F]/[K:F_1]=1$. 所以 $F_1=F$. 因而 K 是 F 上伽罗瓦扩张而且 $G=\mathrm{Gal}(K/F)$. □

引理 3 *设 E/F 为一个有限伽罗瓦扩张, $G=\mathrm{Gal}(E/F)$, 又设 L 为任一中间域. 则 E 是 L 上的伽罗瓦扩张而且 E/L 的伽罗瓦群等于 G 中保持 L 的元素不动的那些自同构组成的子群, 即 $\mathrm{Gal}(E/L)$ 等于 $H=\{\sigma\in G\,|\,\sigma(\alpha)=\alpha$, 对所有 $\alpha\in L\}$.*

证明 设 L_1 为 H 的不动域, 则 $L\subset L_1$. 求证 $L_1=L$. 根据定理 1, $[E:L_1]=|H|$, 因而 $[L_1:F]=[G:H]$. 如果我们能够证明 $[L:F]\geq[G:H]$, 由 $[L:F]\leq[L_1:F]$ 则能推出 $[L:F]=[G:H]=[L_1:F]$. 从而 $L_1=L$. 根据定理 1 即知 E/L 是伽罗瓦扩张, 而且 H 是它的伽罗瓦群. 下面努力证明 $[L:F]\geq[G:H]$. 将 G 按 H 分解成陪集 $G=\sigma_1H\cup\cdots\cup\sigma_rH$, $\sigma_1=1$. H 的元素 τ 在 L 上诱导出恒等映射, 因而属于同一个陪集 σ_iH 的元素 $\sigma_i\tau$ 诱导出同一个 L 到 E 内的 F- 嵌入: $\alpha\mapsto\sigma_i(\alpha),\alpha\in L$. 证明这 r 个嵌入两两不同. 假若 $\sigma_i(\alpha)=\sigma_j(\alpha)$ 对所有 $\alpha\in L$, 那么 $\sigma_j^{-1}\sigma_i(\alpha)=\alpha$ 对所有的 $\alpha\in L$. 于是

$\sigma_j^{-1}\sigma_i \in H$, σ_i 与 σ_j 将属于同一个陪集. 这只有在 $i = j$ 才行. 所以 G 诱导出 r 个不同的 F- 嵌入: $L \to E$. 根据引理 2 推论, $r \leq [L : F]$, 即

$$[G : H] \leq [L : F]. \quad \square$$

伽罗瓦基本定理 设 E/F 为一个有限伽罗瓦扩张, $G = \mathrm{Gal}(E/F)$. 于是

1) 在 G 的子群集 $\{H\}$ 和 E/F 的中间域集 $\{K\}$ 之间存在一个一一对应. 让每个子群 H 对应于它的不动域:

$$H \mapsto \mathrm{Inv}(H),$$

让每个中间域 K 对应于 E 对 K 的伽罗瓦群:

$$K \mapsto \mathrm{Gal}(E/K).$$

于是它们互为逆映射, 即

$$\mathrm{Gal}(E/\mathrm{Inv}(H)) = H,$$
$$\mathrm{Inv}(\mathrm{Gal}(E/K)) = K.$$

2) 上述一一对应是反包含的, 即

$$H_1 \subset H_2 \iff \mathrm{Inv}(H_1) \supset \mathrm{Inv}(H_2).$$

3) 有数量关系

$$[E : \mathrm{Inv}(H)] = |H|,$$
$$[\mathrm{Inv}(H) : F] = [G : H].$$

4) 若子群 H 对应于中间域 K. 则 H 的共轭子群 $\sigma H \sigma^{-1}$ 对应于 K 的共轭子域 $\sigma(K), \sigma \in G$.

5) 设子群 H 对应于中间域 K, 则 H 在 G 内正规当而且仅当 K 在 F 上是伽罗瓦的. 此时将 G 限制到 K 上就得到 K/F 的伽罗瓦群, 即 $\mathrm{Gal}(K/F) \cong G/H$.

1) 中的一一对应称为 **伽罗瓦对应**.

证明

1) $\mathrm{Inv}(H)$ 简记作 K. 由于 H 是 E 的有限自同构群而且 K 是 H 的不动域, 根据定理 1,E 是 K 上的伽罗瓦扩张, 而且 H 是 E/K 的伽罗瓦群, 即 $H = \mathrm{Gal}(E/\mathrm{Inv}(H))$. 其次, 从中间域出发, $\mathrm{Gal}(E/K)$ 简记作 H. 显然 $H \subset G$, 而且 H 是由 G 中所有保持 K 的元素不动的自同构所组成. 根据引理 3, 则 E 是 K 上的伽罗瓦扩张, H 是它的伽罗瓦群. 于是 $\mathrm{Inv}(H) = K$, 即 $K = \mathrm{Inv}(\mathrm{Gal}(E/K))$.

2) 上述一一对应显然是反包含的.

3) 一方面, 由 1) 的证明可知 E 是 $\mathrm{Inv}(H)$ 上的伽罗瓦扩张, H 是它的伽罗瓦群. 根据定理 1, 可知 $[E:\mathrm{Inv}(H)]=|H|$. 另一方面 $[E:F]=|G|, [E:F]=[E:\mathrm{Inv}(H)][\mathrm{Inv}(H):F], |G|=[G:H]|H|$, 从而推出 $[\mathrm{Inv}(H):F]=[G:H]$.

4) 设与 $\sigma(K)$ 对应的子群为 H', 求证 $H'=\sigma H\sigma^{-1}$. 对于任一 $\tau\in H$ 和任一 $\alpha'\in\sigma(K)$, 则 α' 是某个 $\alpha\in K$ 在 σ 下的象, $\sigma(\alpha)=\alpha'$. 于是

$$\begin{aligned}(\sigma\tau\sigma^{-1})(\alpha')&=(\sigma\tau\sigma^{-1})(\sigma(\alpha))=(\sigma\tau\sigma^{-1}\sigma)(\alpha)\\&=\sigma\tau(\alpha)=\sigma(\tau(\alpha))=\sigma(\alpha)=\alpha'.\end{aligned}$$

因而 $\sigma(K)$ 的所有元素在 $\sigma\tau\sigma^{-1}$ 下不动, 于是 $\sigma\tau\sigma^{-1}\in H'$. 这对所有 $\tau\in H$ 都对. 所以 $\sigma H\sigma^{-1}\subset H'$. 反之, 将 $\sigma(K)$ 写成 L, 则 $K=\sigma^{-1}(L)$. 仿照上面的论证可知 $\sigma^{-1}H'(\sigma^{-1})^{-1}\subset H$, 即 $\sigma^{-1}H'\sigma\subset H$. 由此得 $H'\subset\sigma H\sigma^{-1}$. 最后得 $H'=\sigma H\sigma^{-1}$.

E 的两个中间域 K 和 K' 叫做在 F 上**共轭的**, 如果存在一个 $\sigma\in G$ 使得 $K'=\sigma(K)$. 因此得到 4).

5) 设子群 H 与中间域 K 对应. 设 H 在 G 内正规, 于是对所有 $\sigma\in G$ 有 $\sigma H\sigma^{-1}=H$, 从此有 $\sigma(K)=K$. 因而每个 $\sigma\in G$ 限制在 K 上产生 K 的一个 F- 自同构 $\bar\sigma, \bar\sigma\in\mathrm{Gal}(K/F)$. 显然 $\overline{\sigma\tau}=\bar\sigma\cdot\bar\tau$. 于是映射 $\sigma\mapsto\bar\sigma$ 是一个同态 $G\to\mathrm{Gal}(K/F)$, 同态的核 $=H$. 由此诱导出一个单一同态 $G/H\to\mathrm{Gal}(K/F)$. 一方面由 3), $[K:F]=[G:H]$, 另一方面 $|\mathrm{Gal}(K/F))|\le[K:F]$. 由此可知上述同态是一个同构: $G/H\cong\mathrm{Gal}(K/F)$. 最后只须指出 K/F 是一个伽罗瓦扩张. 因为 $[K:F]=|\mathrm{Gal}(K/F)|$, 由定理 1,3) 可知 K/F 是一个伽罗瓦扩张, 而且它的伽罗瓦群同构于 G/H.

反之, 设 K 是 F 上伽罗瓦扩张, 于是 $|\mathrm{Gal}(K/F)|=[K:F]=r$, K 有 r 个不同的 F- 自同构, 即 K 有 r 个不同的到 E 的 F- 嵌入. 求证对于每个 $\sigma\in G$ 有 $\sigma(K)=K$. 假如不然, 有一个 $\sigma\in G$ 使得 $\sigma(K)\neq K$, 那么由 σ 诱导出的 F- 嵌入 $K\to E$ 将与上面的 r 个嵌入都不同, K 将有多于 r 的不同的 F- 嵌入 $K\to E$. 与引理 3 推论抵触. 所以对所有 $\sigma\in G$ 都有 $\sigma(K)=K$. 因而对所有 $\sigma\in G$ 都有 $\sigma H\sigma^{-1}=H$. 所以 H 在 G 内正规. □

下面我们将证明可分正规扩张和伽罗瓦扩张的等价.

引理 4 *设 E/F 是一个有限伽罗瓦扩张, G 是它的伽罗瓦群. 则 E 的任一元素 α 的极小多项式 $g(x)$ 是可分的, 而且 $g(x)$ 的全部根恰好是 α 在 G 作用下得到的全部象集.*

证明 设 $\{\alpha_1=\alpha,\alpha_2,\cdots,\alpha_r\}$ 是 α 在 G 作用下得到的全部象集合 (作为集

合的元素当然 $\alpha_1,\cdots,\alpha_r$ 两两不同). 用 α_i 作一个多项式

$$g_\alpha(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_r).$$

对于任一 $\sigma\in G$, $\sigma(\alpha_1),\cdots,\sigma(\alpha_r)$ 不过是 $\alpha_1,\cdots,\alpha_r$ 的一个排列, 因而 $g_\alpha(x)$ 的系数在 σ 作用下不变, 于是 $g_\alpha(x)$ 是一个 $F[x]$ 中的多项式. 其次证明 $g_\alpha(x)$ 在 F 上不可约. 设 $f(x)$ 为 $F[x]$ 中以 α 为根的任一多项式, $f(x)=x^m+a_1x^{m-1}+\cdots+a_m$. 用 $\sigma\in G$ 作用于 $f(\alpha)=0$ 得

$$\begin{aligned}\sigma(f(\alpha))&=\sigma(\alpha^m+a_1\alpha^{m-1}+\cdots+a_m)\\&=\sigma(\alpha)^m+a_1\sigma(\alpha)^{m-1}+\cdots+a_m=f(\sigma(\alpha))=0.\end{aligned}$$

$\sigma(\alpha)$ 也是 $f(x)$ 的根对所有 $\sigma\in G$, 即每个 α_i 都是 $f(x)$ 的根. 从而 $g_\alpha(x)|f(x)$. 这表明 $g_\alpha(x)$ 在 F 上不可约. 在 F 上以 α 为根的不可约多项式是唯一的 (除常数因子外), 所以 $g_\alpha(x)$ 就是 α 的极小多项式. □

定理 2 *一个有限扩张 E/F 是伽罗瓦扩张当而且仅当 E/F 是一个可分正规扩张. 或者说, 一个有限扩张 E/F 是伽罗瓦扩张当而且仅当 E 是 F 上一个可分多项式的分裂域.*

证明 根据第七章定理 11, 只需证明定理的第一句话. 设 E/F 为一个有限伽罗瓦扩张. 根据引理 4, E 的任一元素 α 的极小多项式 $g_\alpha(x)$ 是可分的, α 为 F 上可分元, 所以 E 是 F 上可分扩张. 而且每个 α 的极小多项式 $g_\alpha(x)$ 在 E 内完全分解成一次因式之积, 所以 E 是 F 上的正规扩张. 反之, 设 E/F 为有限可分正规扩张, G 为它的伽罗瓦群, 求证 G 的不动域等于 F. 设 $\alpha\in E$, $f(x)$ 为 α 在 F 上的极小多项式. 于是 $f(x)$ 在 E 内完全分解. 设 $f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_r)$, 而且 $\alpha_i\neq\alpha_j$ 当 $i\neq j$, $\alpha_1=\alpha$. 若 $\alpha\notin F$, 则 $r>1$. 于是存在一个 F- 同构 $\sigma_1:F(\alpha)\mapsto F(\alpha_2)$ 使得 $\sigma_1(\alpha)=\alpha_2$. 由于 E/F 正规, 根据第七章定理 6, σ_1 可以开拓成 E 的 F- 自同构 σ. 于是 $\sigma\in G$ 而且 $\sigma(\alpha)=\alpha_2\neq\alpha_1$. 因此 $\alpha\notin\mathrm{Inv}(G)$. 所以 $\mathrm{Inv}(G)=F$, E/F 是一个伽罗瓦扩张. □

从此以后, 在处理具体问题的时候, 视情况可以把一个有限伽罗瓦扩张看作一个可分多项式的分裂域或一个可分正规扩张, 使得问题比较容易处理. 下面就是一个例子.

设在基域 F 上给定三个代数扩张 E/F, K/F 和 L/F, 又设有两个 F- 嵌入 $\sigma:E\to L$ 和 $\tau:K\to L$. 那么 L 中同时包含 $\sigma(E)$ 和 $\tau(K)$ 的所有子域的交叫做 E 和 K 的一个 **复合域**, 记作 $\sigma(E)\cdot\tau(K)$. E 和 K 的复合域与嵌入有关. 当嵌入不同时得到的复合域可能不是 F- 同构的. 当 E 是 F 上一个有限正规扩张时, 则 E 和 K 的复合域与嵌入的方式无关, 就是说不论如何嵌入, 它们总是 F- 同构的. 说明如下: 设 E/F 是一个有限正规扩张, 根据第七章定理

7,E 是 F 上一个多项式 $f(x)$ 的分裂域. 在 F- 嵌入 σ 下 $f(x)$ 不变, $\sigma(E)$ 仍然是 $f(x)$ 在 F 上的分裂域. 设 $\sigma(E)=F(\alpha_1,\cdots,\alpha_n)$, $f(x)$ 在 $\sigma(E)$ 内有分解 $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$. 显然有

$$\sigma(E)\subset\tau(K)(\alpha_1,\cdots,\alpha_n)\subset\sigma(E)\cdot\tau(K).$$

又 $\tau(K)\subset\tau(K)(\alpha_1,\cdots,\alpha_n)$. 根据 $\sigma(E)\cdot\tau(K)$ 的定义有

$$\sigma(E)\cdot\tau(K)\subset\tau(K)(\alpha_1,\cdots,\alpha_n).$$

所以 $\sigma(E)\cdot\tau(K)=\tau(K)(\alpha_1,\cdots,\alpha_n)$. $\tau(K)(\alpha_1,\cdots,\alpha_n)$ 是 F 上多项式 $f(x)$ 在 $\tau(K)$ 上的分裂域. 根据第七章定理 6, 对不同的两对 F- 嵌入 $\sigma_i:E\to L$ 和 $\tau_i:K\to L, i=1,2$, 总是有

$$\tau_1(K)(\alpha_1,\cdots,\alpha_n)\cong\tau_2(K)(\alpha_1,\cdots,\alpha_n).$$

即 $\sigma_1(E)\cdot\tau_1(K)\cong\sigma_2(E)\cdot\tau_2(K)$. 因此, 有限正规扩张和任意扩张 K/F 的复合域 $\sigma(E)\cdot\tau(K)$ 与 F- 嵌入 σ,τ 无关, 由 E/F 和 K/F 唯一决定. 以后 $\sigma(E)\cdot\tau(K)$ 简记作 $E\cdot K$. 根据定理 2, 这个结论可表述成: 若 E/F 是 F 上多项式 $f(x)$ 的分裂域, K/F 为任意扩张, 则 E/F 和 K/F 的复合域和 $f(x)$ 在 K 上的分裂域同构.

定理 3 设 E/F 为一个有限伽罗瓦扩张, K/F 为任意域扩张, 于是复合域 $E\cdot K$ 是 K 上伽罗瓦扩张且有

$$\mathrm{Gal}(E\cdot K/K)\cong\mathrm{Gal}(E/E\cap K).$$

而且这个同构可由映射 $\sigma\mapsto\overline{\sigma}=\sigma|E,\sigma\in\mathrm{Gal}(E\cdot K/K)$ 来实现.

证明 根据定理 2 和上面的讨论, E/F 是 F 上一个可分多项式 $f(x)$ 的分裂域. 因而 $E\cdot K$ 是 K 上伽罗瓦扩张. 令 $K_1=E\cap K$. 对于 $\sigma\in\mathrm{Gal}(E\cdot K/K)$, σ 保持 K 的元素不变, 当然也保持 $K_1=E\cap K$ 的元素不变, 而且 σ 保持 $f(x)$ 的根集合变到自身, 因而 σ 保持 E 变到自身. 所以 σ 在 E 上诱导出 E 的一个 K_1-自同构 $\overline{\sigma}=\sigma|E$. 对 $\sigma,\tau\in\mathrm{Gal}(E\cdot K/K)$ 显然有 $\overline{\sigma\tau}=\overline{\sigma}\cdot\overline{\tau}$. 因而映射 $\sigma\mapsto\overline{\sigma}$ 是 $\mathrm{Gal}(E\cdot K/K)$ 到 $\mathrm{Gal}(E/K_1)$ 的一个同态. 其次证明这映射是单一的. 若 $\overline{\sigma}=1$, 则 $\overline{\sigma}$ 保持 $f(x)$ 的每个根不动又保持 K 的元素不动, 当然 σ 保持 $f(x)$ 在 K 上的分裂域, 即 $E\cdot K$ 的元素不动, 因而 $\sigma=1$. 最后证明映射是满的. 这只需证明 $|\mathrm{Gal}(EK/K)|=|\mathrm{Gal}(E/K_1)|$. 由于 EK/K 和 E/K_1 都是伽罗瓦扩张, 根据定理 1, 问题又可转化为证明 $[EK:K]=[E:K_1]$. 由于 E/K_1 有限可分, 根据第七章定理 15 的推论, E 可表成 K_1 上的单扩张, $E=K_1(\theta)$. 设 $g(x)$ 为 θ

在 K_1 上的极小多项式，则 $[E:K_1]=\deg g(x)$. 由于 E/K_1 正规，$g(x)$ 的全部根 $\theta_1=\theta,\theta_2,\cdots,\theta_r$ 全在 E 中. 另一方面 $K(\theta)$ 既包含 K 又包含 $K_1(\theta)=E$, 因而 $K(\theta)$ 包含 K 与 E 的复合 $E\cdot K$, 所以 $E\cdot K=K(\theta)$. 求证 $g(x)$ 也是 θ 在 K 上的极小多项式. 这只需证明 $g(x)$ 在 K 上不可约. 假设 $g(x)=\psi(x)\varphi(x)$ 为在 K 中的任一分解，$\psi(x)$ 和 $\varphi(x)$ 的首项系数为 1,$\psi(x)$ 和 $\varphi(x)$ 的系数都是 $\theta_1,\cdots,\theta_r$ 的多项式，系数为 ±1, 因而 $\psi(x)$ 和 $\varphi(x)$ 的系数全属于 E, 从而它们的系数全属于 $K_1=E\cap K$. 那么 $g(x)=\psi(x)\varphi(x)$ 是 K_1 内的一个分解. 由 $g(x)$ 在 K_1 上的不可约性，从而推出 $\psi(x)=1$ 或 $\varphi(x)=1$. 所以 $g(x)$ 在 K 上也不可约. 由此可知 $[E\cdot K:K]=\deg g(x)$. 总之 $[EK:K]=[E:K_1]$. 综合起来，映射 $\sigma\mapsto\overline{\sigma},\sigma\in\mathrm{Gal}(EK/K)$, 是 $\mathrm{Gal}(EK/K)$ 到 $\mathrm{Gal}(E/K_1)$ 的一个同构. □

§2 多项式的伽罗瓦群

这一节我们按照伽罗瓦原来的想法引进一个多项式的群，并且给出计算它的方法.

设 $f(x)$ 为基域 F 上一个无重根的多项式，次数 $n>0$, E 为 $f(x)$ 的分裂域. 于是 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$, α_i 为 $f(x)$ 的根. E 的元素 α 是 $\alpha_1,\cdots,\alpha_n$ 的多项式，系数在 F 内：$\alpha=\psi(\alpha_1,\cdots,\alpha_n)$. E 的每个 F- 自同构 σ 作用在 α 上有

$$\sigma(\alpha)=\psi(\sigma(\alpha_1),\cdots,\sigma(\alpha_n)). \tag{1}$$

由此可知，σ 由 $\alpha_1,\cdots,\alpha_n$ 的象唯一决定. 特别将 σ 作用于 $f(\alpha_i)=0$ 可知 $f(\sigma(\alpha_i))=0,\sigma(\alpha_i)$ 仍为 $f(x)$ 的根. 因而 σ 引起 $f(x)$ 的根之间的一个置换 $\pi_\sigma:\alpha\mapsto\sigma(\alpha_i)$, $i=1,\cdots,n$. 不同的 σ 引起不同的置换 π_σ, 而且显然，对 $\sigma,\tau\in\mathrm{Gal}(E/F)$ 有 $\pi_\sigma\cdot\pi_\tau=\pi_{\sigma\tau}$. 这样我们得到 $\mathrm{Gal}(E/F)$ 到 $f(x)$ 的根 $\alpha_1,\cdots,\alpha_n$ 的对称群 S_n 的一个单一同态 $\sigma\mapsto\pi_\sigma$. 于是所有 $\pi_\sigma,\sigma\in\mathrm{Gal}(E/F)$ 在 S_n 内形成一个与 $\mathrm{Gal}(E/F)$ 同构的子群 G_f.

定义 4 G_f 叫做多项式 $f(x)$ 在 F 上的 **伽罗瓦群**, 或简称 $f(x)$ 在 F 上的群.

如上所说，每个 $\sigma\in\mathrm{Gal}(E/F)$ 限制到 $f(x)$ 的根上得到置换 π_σ, 反之每个这样得到的置换 π_σ 又可以按自然的方式开拓成 E 的 F- 自同构 $\sigma:\alpha\mapsto\pi_\sigma(\alpha)=\psi(\pi_\sigma(\alpha_1),\cdots,\pi_\sigma(\alpha_n))$. 在这个意义上，$\sigma$ 和 π_σ 可以不加区别. 提起注意的是，并不是 S_n 的每个置换都可以按自然的方式开拓成 E 的 F- 自同构. G_f 有如下的刻画：

定理 4 设 $f(x)\in F[x]$, E/F 和 G_f 如上. 置换 $\pi\in S_n$ 属于 G_f 的充要条件是对每个多项式 $g(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$ 若 $g(\alpha_1,\cdots,\alpha_n)=0$ 恒有

$g(\pi(\alpha_1),\cdots,\pi(\alpha_n))=0$. 即 π 保持 $f(x)$ 的根之间的代数关系总和不变.

证明 必要性由 G_f 的定义即得. 证充分性. 假设 π 满足定理中的条件. 用 π 定义 E 到自身的一个映射 σ 如下: 对每个 $\alpha\in E$, 将 α 表成 $\alpha=\psi(\alpha_1,\cdots,\alpha_n)$. $\psi(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$ 规定

$$\sigma(\alpha)=\psi(\pi(\alpha_1),\cdots,\pi(\alpha_n)).$$

首先, 定义与 α 的表法无关. 设 $\alpha=\varphi(\alpha_1,\cdots,\alpha_n)$ 为另一种表法, $\varphi(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$, 令 $h(x_1,\cdots,x_n)=\psi(x_1,\cdots,x_n)-\varphi(x_1,\cdots,x_n)$, 于是 $h(\alpha_1,\cdots,\alpha_n)=0$ 为 α_i 的一个代数关系, 于是

$$\sigma(h(\alpha_1,\cdots,\alpha_n))=h(\pi(\alpha_1),\cdots,\pi(\alpha_n))=0,$$

即

$$\psi(\pi(\alpha_1),\cdots,\pi(\alpha_n))-\varphi(\pi(\alpha_1),\cdots,\pi(\alpha_n))=0.$$

所以 $\sigma(\alpha)$ 与 α 的表法无关, 由 α 唯一决定. 因而 σ 是 E 到自身的一个映射而且保持 F 的元素不动. 仿上可以证明 σ 保持 E 的加法和乘法. 因而 σ 是 E 的 F- 自同态. 由于 $\sigma(\alpha_1)=\pi(\alpha_1),\cdots,\sigma(\alpha_n)=\pi(\alpha_n)$ 是 $f(x)$ 的全部根, 在 F 上生成 E, σ 是一个满射. 又由于 E 是一域, σ 又是单射, 所以 σ 是 E 的一个 F- 自同构. 由 σ 的定义可知 $\pi=\pi_\sigma$. 所以 $\pi\in G_f$. □

定理 4 表明, 一个 (无重根) 的多项式的伽罗瓦群由它的根的代数关系总和唯一决定.

现在要问 G_f 作为根的置换群在什么条件下是传递的. 假设 G_f 是传递的, 那么 $f(x)$ 的根 $\alpha_1,\cdots,\alpha_n$ 在 G_f 下组成一个传递集. 根据本章 §1 引理 4, 多项式 $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$ 在 F 上不可约. 反之, 设 $f(x)$ 不可约, 同样根据引理 4, 含有 α_1 的传递集恰好是 α_1 的极小多项式 $f(x)$ 的全部根. 因而 $\alpha_1,\cdots,\alpha_n$ 是在 G_f 下含 α_1 的传递集, 这表明 G_f 是传递的.

其次, 我们知道, 根 $\alpha_1,\cdots,\alpha_n$ 的交错群 A_n 是 S_n 的指数为 2 的正规子群, 因而 $A_n\cap G_f$ 也是 G_f 的正规子群, 指数 $[G_f:G_f\cap A_n]\le 2$. 试问这个指数表现在多项式 $f(x)$ 有什么意义? 易知指数 $=1$ 的充要条件是 $G_f\subset A_n$ 即 G_f 不含奇置换. 这与根的交错函数有关系. 根 $\alpha_1,\cdots,\alpha_n$ 的交错函数是指 $\Delta=\prod\limits_{i<j}(\alpha_i-\alpha_j)$. 将 $\alpha_1,\cdots,\alpha_n$ 看作根的自然顺序, 若 $i<j$, 则 α_j,α_i 看作一个逆序. 设置换 $\pi\in G_f$ 有 r 个逆序. π 作用在 Δ 上不难说明

$$\pi(\Delta)=\prod_{i<j}(\pi(\alpha_i)-\pi(\alpha_j))=(-1)^r\prod_{i<j}(\alpha_i-\alpha_j),$$

得

$$\pi(\Delta) = (-1)^r\Delta.$$

若特征 $\chi(F) = 2$, 则 $-1 = 1, \pi(\Delta) = \Delta$, 对所有 $\pi \in G_f$, 因而 Δ 恒属于基域 F, 设 $\chi(F) \neq 2$, 则 $\pi(\Delta) = \Delta$ 的充要条件是 π 为偶置换. 因此在伽罗瓦对应下中间域 $K = F(\Delta)$ 与子群 $G_f \cap A_n$ 对应.

Δ^2 记作 $D(f)$, 叫做 $f(x)$ 的判别式. $D(f)$ 恒属于 F. 综上所述得到

定理 5 *设 G_f 为一个 n 次无重根多项式 $f(x)$ 在 F 上的伽罗瓦群. 于是*

1) G_f 是传递的充要条件是 $f(x)$ 在 F 上不可约.

2) 设 $\chi(F) \neq 2$, 则 G_f 只含偶置换的充要条件是 $f(x)$ 的判别式 $D(f)$ 在 F 内可开平方. 令 $\Delta = \sqrt{D(f)}$, $K = F(\Delta)$, 则 $\mathrm{Gal}(E/K) = G_f \cap A_n$. □

多项式 $f(x)$ 的判别式是根的对称函数, 可以表成 $f(x)$ 的系数的多项式. 将几个低次的 $f(x)$ 的判别式写在下面:

$$f(x) = x^2 + bx + c, \quad D(f) = b^2 - 4c,$$

$$f(x) = x^3 + ax^2 + bx + c, \quad D(f) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

若 $\chi(F) \neq 3$, 则经过一个替换 $x = y - \dfrac{a}{3}$ 将 $f(x)$ 化为下列形状

$$g(y) = y^3 + py + q,$$

此时

$$D(g) = -4p^3 - 27q^2 = D(f).$$

当 $\chi(F) \neq 2$ 时, 一个四次多项式 $x^4 + ax^3 + bx^2 + cx + d$ 经过一个替换 $x = y - \dfrac{a}{4}$ 可化为

$$g(y) = y^4 + py^2 + qy + r.$$

此时,

$$D(g) = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3 = D(f).$$

利用定理 5 比较容易地定出低次无重根多项式的群.

域 F 上二次多项式 $f(x) = x^2 + bx + c$ 的群只有两种可能: 若 $f(x)$ 不可约, 则 G_f 为二文字的传递群即 S_2. 否则 G_f 为单位元群.

域 F 上三次多项式 $f(x) = x^3 + ax^2 + bx + c$ 的群有多种可能. 根据定理 5 完全可以决定. 若 $f(x)$ 在 F 内完全分解 $f(x) = (x-\alpha)(x-\beta)(x-\gamma)$, 则 G_f 为单位元群. 若 $f(x) = (x^2 + rx + s)(x - \gamma)$, 而 $x^2 + rx + s$ 在 F 上不可约, 那么 G_f 等于 S_3 的子群 S_2. S_2 表示 $x^2 + rx + s$ 的两根的对称群. 设 $\chi(F) \neq 2$

而且 $f(x)$ 在 F 上不可约，则 $f(x)$ 的群 G_f 是三文字的传递群，即 $G_f=S_3$ 或 A_3. 进一步计算 $f(x)$ 的判别式 D. 若 D 在 F 内不能开平方，则 $G_f=S_3$; 否则 $G_f=A_3$.

F 上四次多项式 $f(x)$ 的群有更多的可能性. 若 $f(x)$ 可约，则可归结到上面的情况去讨论. 设 $f(x)$ 在 F 上不可约. 此时 G_f 是四文字的传递群， G_f 的阶是 4 的倍数有 4,8,12, 和 24 四种可能. 而 S_4 中阶为 4 的倍数的传递子群由 S_4, A_4, 西罗 2- 子群，四元群 $V=\{e,(12)(34),(13)(24),(14)(23)\}$ 和循环群 $Z=\langle(1234)\rangle$ 五种. 因而 G_f 只有五种可能. 应用定理 5,2) 还不足以决定 G_f. 除了定理 5 以外还需要引进 $f(x)$ 的根的新的函数. 定理 5 中的 Δ 是一个二值函数，就是说 Δ 在 G_f 的作用下一般出现两个值 Δ 和 $-\Delta$. 我们还要引进根的三值函数. 以下一直假设 $\chi(F)\neq 2$ 和 $f(x)=x^4+px^2+qx+r$ 在 F 上不可约. 设 $E=F(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$ 为 $f(x)$ 的分裂域， α_i 为 $f(x)$ 的根. 在 E 中取

$$\alpha=(\alpha_1+\alpha_2)(\alpha_3+\alpha_4), \beta=(\alpha_1+\alpha_3)(\alpha_2+\alpha_4), \gamma=(\alpha_1+\alpha_4)(\alpha_2+\alpha_3).$$

由计算可知，每个 $\pi\in G_f$ 作用于 α,β,γ 只能引起 α,β,γ 的一个排列. 因此，以 α,β,γ 为根作一个多项式

$$g(x)=(x-\alpha)(x-\beta)(x-\gamma)=x^3+b_1x^2+b_2x+b_3,$$

$g(x)$ 的系数 b_i 在 G_f 的作用下不变，从而 $b_i\in F$. $g(x)$ 是 F 上一个三次多项式. 令 $K=F(\alpha,\beta,\gamma)$. 则 K 是 E/F 的一个中间域而且是 $g(x)$ 的分裂域. 因而 K/F 是一个伽罗瓦扩张. 应用对称函数基本定理计算 $g(x)$ 的系数得

$$\begin{aligned} b_1&=-(\alpha+\beta+\gamma)=-2p,\\ b_2&=\alpha\beta+\alpha\gamma+\beta\gamma=p^2-4r,\\ b_3&=-\alpha\beta\gamma=q^2. \end{aligned}$$

因而 $g(x)$ 的系数可以从 $f(x)$ 的系数算出来. 有趣的是 $g(x)$ 的判别式等于 $f(x)$ 的判别式. 事实上

$$\begin{aligned} \beta-\alpha&=(\alpha_3-\alpha_2)(\alpha_4-\alpha_1),\\ \gamma-\alpha&=(\alpha_3-\alpha_1)(\alpha_4-\alpha_2),\\ \gamma-\beta&=(\alpha_2-\alpha_1)(\alpha_4-\alpha_3). \end{aligned}$$

于是得 $D(g)=D(f)$. 由于 $f(x)$ 可分， $D(f)\neq 0$, 从而 $D(g)\neq 0$, α,β,γ 两两不同. 在伽罗瓦对应下设 G_f 的子群 H 与 K 对应. 求证

$$\mathrm{Gal}(E/K)=H=G_f\cap V,$$

其中 $V=\{1,(\alpha_1\alpha_2)(\alpha_3\alpha_4),(\alpha_1\alpha_3)(\alpha_2\alpha_4),(\alpha_1\alpha_4)(\alpha_2\alpha_3)\}$.

因为 G_f 中每个置换必属于下列五种类型之一：

$$e,\ (\alpha_1\alpha_2)(\alpha_3\alpha_4),(\alpha_1\alpha_2),(\alpha_1\alpha_2\alpha_3),(\alpha_1\alpha_2\alpha_3\alpha_4),$$

其中前两种属于 V 而后三种则不属于 V. 同一种类型的置换对 α,β,γ 的作用是相似的 (因为 $\alpha_1,\cdots,\alpha_4$ 在 α,β,γ 中处在对称的地位) 因而只需考察上面五个置换对 α,β,γ 的作用就够了. 头两个都分别保持 α,β,γ 不动, 因而保持 K 的元素不动, 所以属于 H. 而 (α_1,α_2) 对换 β 和 γ, $(\alpha_1,\alpha_2,\alpha_3)$ 将 α,β,γ 变成 γ,α,β, $(\alpha_1\alpha_2\alpha_3\alpha_4)$ 对换 α 和 γ. 由于 α,β,γ 两两不等, 由此可知后三类不属于 H. 所以 $G_f\cap V=H=\mathrm{Gal}(E/K)$.

如上构造出的三次多项式 $g(x)$ 叫做四次不可约多项式 $f(x)$ 的 **预解式**. 我们可以根据 $g(x)$ 的群定出 $f(x)$ 的群. 兹分情况讨论如下:

1) $g(x)$ 在 F 上不可约而且判别式 $D(g)$ 在 F 内不能开平方. 根据三次多项式的群的讨论, 可知 $\mathrm{Gal}(K/F)\cong S_3$. 特别 $[G_f:H]=6$. 从而 $3\,|\,|G_f|$. 已知 $4\,|\,|G_f|$, 所以 G_f 的阶为 12 或 24. 由于 S_4 只有唯一的一个 12 阶子群 A_4, 全由偶置换组成, 而 G_f 含有奇置换, 所以 G_f 只能是 S_4.

2) $g(x)$ 在 F 上不可约但 $\sqrt{D(g)}\in F$. 此时, 有 $\sqrt{D(f)}\in F$, G_f 只含偶置换, $G_f\subset A_4$. 另一方面, 根据三次多项式的结果, $\mathrm{Gal}(K/F)\cong A_3$, 从而 $3\,|\,|G_f|$. 由于 $4\,|\,|G_f|$, 有 $12\,|\,|G_f|$, 所以 $G_f=A_4$.

3) $g(x)$ 在 F 内分解成一个 2 次不可约因式和一个一次因式之积. 此时 $[K:F]=[G_f:H]=2$. 由于 $|H|\le|V|=4$, 有 $|G_f|\le 8$. 因而 G_f 的阶只能是 4 或 8, 而 $[E:K]$ 只能是 2 或 4. 若 $f(x)$ 在 K 上不可约, 则 $[E:K]=4$, 从而 $|G_f|=8$. G_f 是 S_4 的一个 8 阶传递子群. 但 S_4 的 8 阶子群只有一个共轭类即西罗 2- 子群, 而且传递. 这类子群与二面体群 D_4 同构. 所以 $G_f=\langle(12),(1324)\rangle\cong D_4$. 设 $f(x)$ 在 K 上可约, 则 $[E:K]<4$, $|G_f|<8$. 此时 G_f 是一个 4 阶传递子群. 但是 S_4 的 4 阶传递子群有两个共轭类即四元群 $V=\langle(12)(34),(13)(24)\rangle$, 和循环群 $Z=\langle(1234)\rangle$. 为了进一步决定 G_f 需要计算 $g(x)$ 的判别式. 设 $g(x)$ 的三根中 α,β 适合 2 次不可约多项式 $\psi(x)\in F[x]$, 而 $\gamma\in F$. 于是

$$\begin{aligned}D(g)=&[(\gamma-\alpha)(\gamma-\beta)(\beta-\alpha)]^2=\psi(\gamma)^2(\beta-\alpha)^2\\=&\psi(\gamma)^2D(\psi),\end{aligned}$$

其中 $\psi(\gamma)\in F$. 由于 $\psi(x)$ 不可约, $\sqrt{D(\psi)}\notin F$, 因而 $\sqrt{D(g)}\notin F$. 从而 G_f 含有奇置换. 于是 G_f 只能与循环群 $\langle(1234)\rangle$ 同构.

4) $g(x)$ 在 F 内分解成一次因式之积即 α,β,γ 全属于 F. 此时 $K=F$, $H=G_f$, 因而 $|G_f|\le 4$. 但是 $4\,|\,|G_f|$, 所以 $|G_f|=4$. 从 $G_f\cap V=H=G_f$ 推出

$G_f = V$.

综上所述得到下列事实：（将 $f(x)$ 的根 $\alpha_1, \cdots, \alpha_4$ 简记作 $1, \cdots, 4$.）

定理 6 设域 F 的特征 $\neq 2$, 又设 $f(x)$ 为域 F 上一个 4 次不可约多项式. $g(x)$ 为它的 3 次预解式， K/F 为 $g(x)$ 的分裂域. 于是

1) 若 $g(x)$ 不可约而且 $\sqrt{D(g)} \notin F$, 则 $G_f = S_4$.

2) 若 $g(x)$ 不可约而且 $\sqrt{D(g)} \in F$, 则 $G_f = A_4$.

3) 若 $g(x)$ 有一个 2 次不可约因式，而且 $f(x)$ 在 K 上不可约，则 $G_f \cong \langle(13), (1234)\rangle$.

4) 若 $g(x)$ 有一个 2 次不可约因式, 而且 $f(x)$ 在 K 上可约, 则 $G_f \cong \langle(1234)\rangle$.

5) 若 $g(x)$ 完全可分解成一次因式之积，则 $G_f = \langle(12)(34), (13)(24)\rangle$. □

应用上面的结果来计算几个整系数多项式在有理数域 $\mathbf{Q}$ 上的群.

例 1 $f(x) = x^4 + 2x^2 + 4x + 2$.

根据艾森斯坦判别法可知， $f(x)$ 在 $\mathbf{Q}$ 上不可约，它的三次预解式 $g(x) = x^3 - 4x^2 - 4x + 16$. 而且 $g(x) = (x-4)(x-2)(x+2)$, 所以 $f(x)$ 的群 G_f 为 $V = \{e, (12)(34), (13)(24), (14)(23)\}$.

例 2 $f(x) = x^4 + 8x + 12$.

读者不难验证 $f(x)$ 在 $\mathbf{Q}$ 上不可约. 它的三次预解式 $g(x) = x^3 - 48x + 8^2$. $g(x)$ 在 $\mathbf{Q}$ 上也不可约. 但 $D(g) = -4 \cdot (-48)^3 - 27 \cdot 8^4 = 2^{12} \cdot 3^4$ 是一个平方数，所以 $f(x)$ 的群为交错群 A_4.

例 3 $f(x) = x^4 + 2x^2 + 2$.

$f(x)$ 在 $\mathbf{Q}$ 上不可约. 它的三次预解式 $g(x) = x^3 - 4x^2 - 4x = x(x^2 - 4x - 4)$, $x^2 - 4x - 4$ 在 $\mathbf{Q}$ 上不可约. 因而 $f(x)$ 的群 G_f 或同构于 S_4 的西罗 2- 子群或同构于循环群 $Z = \langle(1234)\rangle$. $x^2 - 4x - 4$ 的根为 $2 \pm 2\sqrt{2}$, $g(x)$ 的分裂域为 $K = \mathbf{Q}(\sqrt{2})$. 由于 $f(x)$ 没有实根而 K 是实子域， $f(x)$ 在 K 上只能分解成两个 2 次因式之积. 又因为 $f(x)$ 只含偶次项， $f(x)$ 在 K 上只能分解成如下形式

$$f(x) = (x^2 + ax + b)(x^2 - ax + b).$$

比较两边的系数得 $b = \pm\sqrt{2}, a^2 = \pm 2\sqrt{2} - 2$. 由于 $a \in K$, $a^2 > 0$, 只能有 $a^2 = 2\sqrt{2} - 2 = 2(\sqrt{2} - 1)$. 2 在 K 内能开平方 $2 = (\sqrt{2})^2$ 但 $\sqrt{2} - 1$ 则不能，因而方程 $a^2 = 2\sqrt{2} - 2$ 在 K 内无解. 所以 $f(x)$ 在 K 上不可约. 根据前面的讨论， $f(x)$ 的群 G_f 为 S_4 的一个西罗 2- 子群.

$G_f = S_4$ 和 $G_f \cong \langle(1234)\rangle$ 的 4 次不可约整系数多项式的例子以后可以见到. 高次无重根的多项式的伽罗瓦群的一般计算方法将在以后给出. 下面我们进一步给出例 3 中的群 G_f 的具体形式并写出子群和子域的伽罗瓦对应.

例 4 $f(x)=x^4+2x^2+2$, $G_f\cong D_4$. 先具体写出 G_f. 由于 $f(x)$ 只有偶次项, 若 α 为 $f(x)$ 的一根, 则 $-\alpha$ 也是它的根. 因此不妨设 $f(x)$ 的根为 $\alpha,-\alpha,\beta$ 和 $-\beta$. 于是 α^2 和 β^2 为 x^2+2x+2 的根. 解出得 $\alpha^2=i-1,\beta^2=-i-1$. 不妨记 $\alpha=\sqrt{i-1},\beta=\sqrt{-i-1}$. 设 $E/\mathbf{Q}$ 为 $f(x)$ 的分裂域, 则 $\mathbf{Q}(\alpha)$ 和 $\mathbf{Q}(\beta)$ 为 E 的中间域, 且

$$E=\mathbf{Q}(\alpha,\beta),\mathbf{Q}(\alpha)\cap\mathbf{Q}(\beta)=\mathbf{Q}(\alpha^2)=\mathbf{Q}(\beta^2)=\mathbf{Q}(i),$$

$[E:\mathbf{Q}(i)]=4$, E 的每个自同构都引起 $\mathbf{Q}(i)$ 的自同构. 反之, $\mathbf{Q}(i)$ 的每个自同构在 E 上有四个不同的开拓. 另一方面, α 和 β 在 $\mathbf{Q}(i)$ 上的极小多项式分别为 $x^2-(i-1)$ 和 $x^2-(-i-1)$. $\mathbf{Q}(i)$ 的自同构在 E 上的每一个开拓由 α 和 β 的象唯一决定. 下面具体写出 E 的 8 个自同构. 为简单起见, $\alpha,-\alpha,\beta,-\beta$ 分别记作 1,2,3,4.

$\mathbf{Q}(i)$ 的恒等自同构在 E 上有四个开拓, 它们都保持 i 不动, 也就保持 $x^2-(i-1)$ 和 $x^2+(i+1)$ 不动. 因而它们只能引起 $\alpha,-\alpha$ 之间的置换和 $\beta,-\beta$ 之间的置换, 而且这两部分置换是独立的, 所以这四个开拓用根的置换表示就是

$$e,\ (12),\ (34),\ (12)(34).$$

$\mathbf{Q}(i)$ 的自同构 $a+bi\mapsto a-bi,a,b\in\mathbf{Q}$ 将 i 变成 $-i$, 因而它在 E 上的四个开拓是将 $x^2-(i-1)$ 的根和 $x^2-(-i-1)$ 的根互换. 即将 α 变成 β 或 $-\beta$, 同时将 β 变成 α 或 $-\alpha$ 而且互不依赖. 因而它在 E 上的四个开拓用根的置换表出就是

$$(13)(24),\ (14)(23),\ (1324),\ (1423).$$

这样 G_f 由上面 8 个置换组成. G_f 除单位元群和本身外有三个 4 阶子群和五个 2 阶子群:

4 阶子群: $V=\{e,(12)(34),(13)(24),(14)(23)\}$,

$Z=\langle(1324)\rangle$,

$V_1=\{e,(12),(34),(12)(34)\}$

2 阶子群: $\langle(12)\rangle,\langle(34)\rangle,\langle(12)(34)\rangle,\langle(13)(24)\rangle$ 和 $\langle(14)(23)\rangle$.

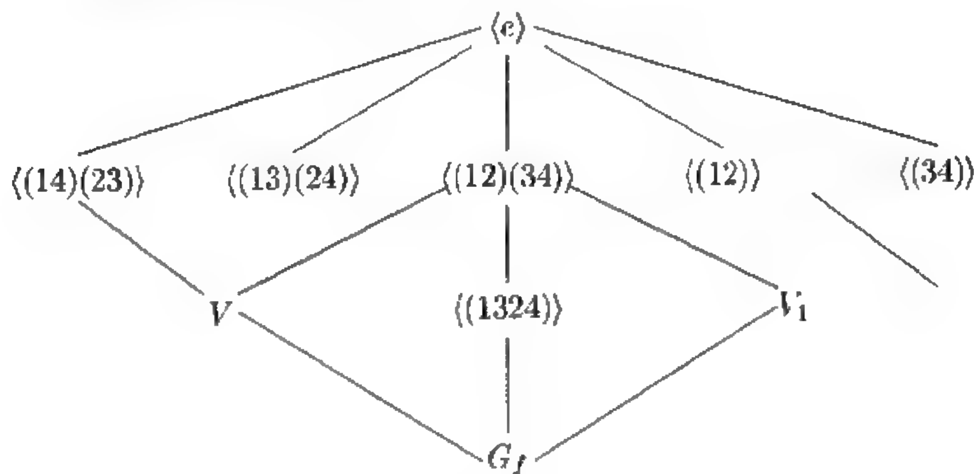
找出与上述子群对应的子域. 首先, 根据上面的 G_f 构造可知 $\mathbf{Q}(i)\subset\mathrm{Inv}(V_1)$. 由于 $[E:\mathbf{Q}(i)]=|V_1|=4$. 根据伽罗瓦基本定理, $\mathrm{Inv}(V_1)=\mathbf{Q}(i)$. 由于 $\alpha^2\beta^2=2,\alpha,\beta$ 不妨如此选择使得 $\alpha\beta=\sqrt{2}$. 显然 $\alpha\beta=\sqrt{2}$ 是 V 的不动元, 因而 $\mathbf{Q}(\sqrt{2})=\mathbf{Q}(\alpha\beta)\subset\mathrm{Inv}(V)$. 由于 $[E:\mathbf{Q}(\sqrt{2})]=|V|=4$. 同理有 $\mathrm{Inv}(V)=\mathbf{Q}(\sqrt{2})$. 注意 (1324) 将 i 变成 $-i$, 而且将 $\alpha\beta=\sqrt{2}$ 变成 $-\alpha\beta=-\sqrt{2}$, 因而 $i\cdot\sqrt{2}=\sqrt{-2}$ 在 (1324) 下不动. $\sqrt{-2}$ 是 Z 的一个不动元. 于是 $\mathbf{Q}(\sqrt{-2})=$

$\mathbf{Q}(\alpha\beta(\alpha^2-\beta^2))\subset \mathrm{Inv}(Z)$. $[E:\mathbf{Q}(\sqrt{-2})]$ 等于 Z 的阶，可知 $\mathrm{Inv}(Z)=\mathbf{Q}(\sqrt{-2})$. 其次来定出二阶子群的不动域. 根据伽罗瓦基本定理可知，2 阶子群的不动域都是 $\mathbf{Q}$ 上 4 次域. (注意 $[E:\mathbf{Q}]=8$) 首先显然有

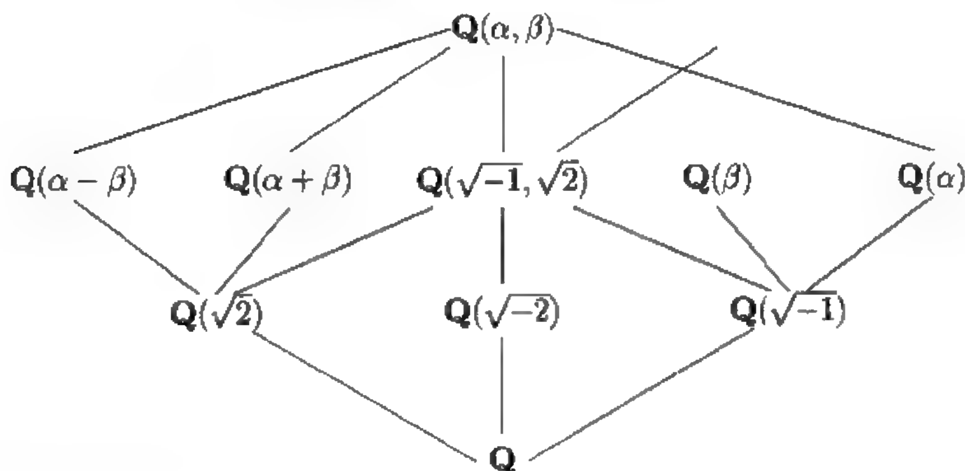
$$\mathrm{Inv}(\langle(12)\rangle)=\mathbf{Q}(\beta),\mathrm{Inv}(\langle(34)\rangle)=\mathbf{Q}(\alpha).$$

其次由于 $\langle(12)(34)\rangle=V\cap Z$, 根据伽罗瓦基本定理 $\langle(12)(34)\rangle$ 的不动域包括 V 和 Z 的不动域的复合域 $\mathbf{Q}(\sqrt{2})\cdot\mathbf{Q}(\sqrt{-2})=\mathbf{Q}(\sqrt{2},\sqrt{-2})=\mathbf{Q}(\sqrt{2},i)$. 而且根据基本定理 3), 有 $\mathrm{Inv}(\langle(12)(34)\rangle)=\mathbf{Q}(\sqrt{2},i)$. 最后定出 $\langle(13)(24)\rangle$ 和 $\langle(14)(23)\rangle$ 的不动域. 首先 $\alpha+\beta$ 是 $(13)(24)$ 的不动元，因而 $\mathbf{Q}(\alpha+\beta)\subset\mathrm{Inv}(\langle(13)(24)\rangle)$. 决定 $\mathbf{Q}(\alpha+\beta)$ 的次数. $(\alpha+\beta)^2=\alpha^2+\beta^2+2\alpha\beta=2+2\sqrt{2}=2(1+\sqrt{2})$. 由此可知 $\mathbf{Q}(\sqrt{2})\subset\mathbf{Q}(\alpha+\beta)$. 又因 2 在 $\mathbf{Q}(\sqrt{2})$ 内是一个平方数 $2=(\sqrt{2})^2$, 而 $1+\sqrt{2}$ 在 $\mathbf{Q}(\sqrt{2})$ 内不能开平方，可知 $\alpha+\beta\notin\mathbf{Q}(\sqrt{2}),[\mathbf{Q}(\alpha+\beta):\mathbf{Q}(\sqrt{2})]=2$, 从而 $[\mathbf{Q}(\alpha+\beta):\mathbf{Q}]=4$. 所以 $\mathrm{Inv}(\langle(13)(24)\rangle)=\mathbf{Q}(\alpha+\beta)$. 其次令 $\tau=(1234)$, 有 $(14)(23)=\tau(13)(24)\tau^{-1}$. 根据伽罗瓦基本定理，$\mathbf{Q}(\tau(\alpha+\beta))=\mathbf{Q}(\beta-\alpha)$ 是 $\tau\langle(13)(24)\rangle\tau^{-1}=\langle(14)(23)\rangle$ 的不动域.

现将 $\mathbf{Q}(\alpha,\beta)$ 的子域和它的群 G_f 的子群之间的伽罗瓦对应用图表示出来，用 1,2,3,4 分别表示 $f(x)$ 的根 $\alpha,-\alpha,\beta$ 和 $-\beta$.



其中 $V=\langle(12)(34),(13)(24)\rangle, V_1=\langle(12),(34)\rangle$.



§3 有限域的伽罗瓦群及其子域

先回忆一下第七章所得到的结果. 一个有限域 F 的特征是一个素数, 设为 p. 于是 F 包含素域 $\mathbf{F}_p = \mathbf{Z}/(p)$. 设 $[F:\mathbf{F}_p] = n$, 则 F 的元素个数为 p^n. 而且 F 是 $x^{p^n} - x$ 在 $\mathbf{F}_p$ 上的分裂域, F 恰由 $x^{p^n} - x$ 的全部根组成. 这样, F 由它的特征 p 和次数 $[F:\mathbf{F}_p]$ 唯一决定. F 作为加法群是一个初等 p 群, 所谓 **初等 p 群** 就是不变量为 $p, p, \cdots, p$ 的有限阿贝尔群. $F^* = F - \{0\}$ 作为乘法群是一个循环群. 它的生成元的个数等于 $\varphi(p^n - 1)$. F 可由 F^* 的生成元在 $\mathbf{F}_p$ 上生成, 因而是 $\mathbf{F}_p$ 上的单扩张. 反之, F 的本原元素的个数等于

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

(见第七章习题 22) 可见 $F/\mathbf{F}_p$ 的本原元素比 F^* 的生成元多得多.

由于 F 是可分多项式 $x^{p^n} - x$ 在 $\mathbf{F}_p$ 上的分裂域, 根据定理 2, $F/\mathbf{F}_p$ 是一个伽罗瓦扩张. 记 $G = \mathrm{Gal}(F/\mathbf{F}_p)$. 根据第七章, F 有一个弗罗贝尼乌斯自同构 σ:

$$\sigma(\alpha) = \alpha^p, \quad \alpha \in F.$$

定义 5 如果一个伽罗瓦扩张 E/K 的伽罗瓦群是一个循环群, 则 E/K 叫做一个 **循环扩张**.

定理 7 *p^n 元有限域 F 是素域 $\mathbf{F}_p$ 上的循环扩张. 而且它的伽罗瓦群由它的弗罗贝尼乌斯自同构 σ 生成.*

证明 首先指出, 循环群 $\langle\sigma\rangle$ 的不动域等于 $\mathbf{F}_p$. 设 $\alpha \in F$ 为 σ 的一个不动元: $\sigma(\alpha) = \alpha$, 于是 $\alpha^p = \alpha$. α 是 $x^p - x$ 的一根, 因而 $\alpha \in \mathbf{F}_p$. 所以 $\mathrm{Inv}(\langle\sigma\rangle) \subset \mathbf{F}_p$. 反之, 因为 $\mathbf{F}_p$ 是一个素域, $\mathbf{F}_p = \{re \mid r = 0, 1, \cdots, p-1\}$ 是由单位元素 e 生

成的，于是 $\sigma(r\cdot e)=r\sigma(e)=r\cdot e$, re 在 σ 下不动，所以 $\mathbf{F}_p\subset \mathrm{Inv}(\langle\sigma\rangle)$. 总之，$\mathrm{Inv}(\langle\sigma\rangle)=\mathbf{F}_p$. 根据定理 1,$\langle\sigma\rangle=\mathrm{Gal}(F/\mathbf{F}_p)$. 所以 $F/\mathbf{F}_p$ 是一个循环扩张.

□

p^n 元有限域由它的元素个数 p^n 唯一决定，因而 p^n 元有限域可以明确地记成 $\mathbf{F}_{p^n}$ 或 $\mathbf{F}_q, q=p^n$. 下面我们根据伽罗瓦基本定理找出 $\mathbf{F}_{p^n}/\mathbf{F}_p$ 的全部中间域. 由于 $\mathbf{F}_{p^n}$ 的每个子域都包含素域 $\mathbf{F}_p$, 因而实际上是找出 $\mathbf{F}_{p^n}$ 的全部子域. 由于 $\mathbf{F}_{p^n}/\mathbf{F}_p$ 的伽罗瓦群是 n 阶循环群 $\langle\sigma\rangle$, $\langle\sigma\rangle$ 的子群我们是清楚的. 对 n 的每个因子 d, n 阶循环群 $\langle\sigma\rangle$ 有一个而且只有一个 $\dfrac{n}{d}$ 阶子群，它由 σ^d 生成. 因而 $\langle\sigma^d\rangle, d|n$, 就是 $\langle\sigma\rangle$ 的全部子群.

定理 8 1) *对 n 的每个正因子 d, 有限域 $\mathbf{F}_{p^n}$ 有一个而且只有一个 p^d 元子域 $\mathbf{F}_{p^d}$; 它是 $x^{p^d}-x$ 的分裂域. 在伽罗瓦对应下，$\mathbf{F}_{p^d}$ 与子群 $\langle\sigma^d\rangle$ 对应.*

2) $\mathbf{F}_{p^d}/\mathbf{F}_p$ 的伽罗瓦群与 $\langle\sigma\rangle/\langle\sigma^d\rangle$ 同构. 令 $\bar\sigma=\sigma|\mathbf{F}_{p^d}$, 则 $\mathrm{Gal}(\mathbf{F}_{p^d}/\mathbf{F}_p)=\langle\bar\sigma\rangle$, $\bar\sigma$ 为 $\mathbf{F}_{p^d}$ 的弗罗贝尼乌斯自同构.

3) 子域 $\mathbf{F}_{p^d}$ 包含 $\mathbf{F}_{p^{d'}}$ 的充要条件是 $d'|d$. 因此有

$$\mathbf{F}_{p^d}\cap\mathbf{F}_{p^{d'}}=\mathbf{F}_{p^r},\quad r=(d,d'),$$
$$\mathbf{F}_{p^d}\cdot\mathbf{F}_{p^{d'}}=\mathbf{F}_{p^m},\quad m=[d,d'].$$

证明 1) 设 $\alpha\in\mathbf{F}_{p^n}$ 为 σ^d 的任一不动元，于是 $\sigma^d(\alpha)=\alpha^{p^d}=\alpha$, α 为 $x^{p^d}-x$ 的一根. 反之，由于 $d|n, x^{p^d}-x|x^{p^n}-x$. $x^{p^d}-x$ 在 $\mathbf{F}_{p^n}$ 内有 p^d 个不同的根，而且每个根 β 有 $\sigma^d(\beta)=\beta^{p^d}=\beta$, β 是 σ^d 的不动元. 所以 $\mathrm{Inv}(\langle\sigma^d\rangle)$ 恰好由 $x^{p^d}-x$ 在 $\mathbf{F}_{p^n}$ 内的全部根组成. 即 $\mathrm{Inv}(\langle\sigma^d\rangle)=\mathbf{F}_{p^d}$.

2) 由伽罗瓦基本定理即得.

3) 根据伽罗瓦基本定理有

$$\mathbf{F}_{p^d}\supset\mathbf{F}_{p^{d'}}\iff\langle\sigma^d\rangle\subset\langle\sigma^{d'}\rangle\iff d'|d.$$

其余两条显然. □

对于任意两个有限域 $\mathbf{F}_{p^n}$ 和 $\mathbf{F}_{p^m}$, 若 $m|n$, 则由定理 8,$\mathbf{F}_{p^n}$ 含有一个 p^m 元子域与 $\mathbf{F}_{p^m}$ 同构. 另一方面，由于 $\mathbf{F}_{p^n}$ 和 $\mathbf{F}_{p^m}$ 都是 $\mathbf{F}_p$ 上的伽罗瓦扩张，根据定理 3, $\mathbf{F}_{p^n}$ 与 $\mathbf{F}_{p^m}$ 的复合域等于 $\mathbf{F}_{p^n}$. 这就是说，只要 $m|n$, $\mathbf{F}_{p^m}$ 就可以看作 $\mathbf{F}_{p^n}$ 的子域. 而且 $\mathbf{F}_{p^n}/\mathbf{F}_{p^m}$ 的伽罗瓦群等于 $\langle\sigma^m\rangle$, 其中 σ 是 $\mathbf{F}_{p^n}$ 的弗罗贝尼乌斯自同构.

定理 7 和定理 8 是将 $\mathbf{F}_{p^n}$ 作为素域 $\mathbf{F}_p$ 上的伽罗瓦扩张所得到的结论. 若将 $\mathbf{F}_{p^n}$ 看作它的任一个子域 $\mathbf{F}_{p^m}$ 上的伽罗瓦扩张，则定理 7 和定理 8 可以推广到 $\mathbf{F}_{p^n}/\mathbf{F}_{p^m}$. 这种推广读者自己可以作出来.

最后，根据第七章定理 13 可知，当 $(n,p)=1$ 时，x^n-1 在 $\mathbf{F}_p$ 上的分裂域 $\mathbf{F}_p(\zeta)$ 是 $\mathbf{F}_p$ 上 m 次扩张，其中 m 为 $p\,(\mathrm{mod}\,n)$ 的指数，ζ 为一个本原 n 次单位根．因而 $\mathbf{F}_p(\zeta)/\mathbf{F}_p$ 是 m 次循环扩张．设 K 为 $\mathbf{F}_p$ 上任一域扩张．根据定理 3, x^n-1 在 K 上的分裂域 $K(\zeta)$ 即 $\mathbf{F}_p(\zeta)\cdot K$ 是 K 上的一个循环扩张，它的次数 $[K(\zeta):K]$ 是 m 的因子．

§4 方程的根可用根式解的判别准则

这一节将揭示特征 0 的域 F 上任一无重根的多项式 $f(x)$ 的群和 $f(x)$ 的根可用根式解之间的深刻的联系．这是天才数学家伽罗瓦所取得的完美的成果．

定义 6 如果一个有限扩张 K/F 是一个单扩张 $K=F(\alpha)$ 而且 $\alpha^n=a\in F, n=[K:F]$, 则 K/F 叫做一个 **单根式扩张**．一般说来，如果一个有限扩张 K/F 可以插进一串中间域

$$F=F_0\subset F_1\subset\cdots\subset F_r=K, \tag{1}$$

使得每个 $F_{i+1}/F_i,\ i=0,\cdots,r-1$ 都是单根式扩张，则 K/F 叫做 **根式扩张**, 而 (1) 叫做 K/F 的一个 **根式扩张链**.

定义 7 若域 F 上一个多项式 $f(x)$ 的分裂域 E 包含在 F 上一个根式扩张 K 中，则称 $f(x)$ 的根在 F 上 **可用根式解**.

例 1 有理数域 $\mathbf{Q}$ 上二次多项式 $f(x)=x^2-3x+5$ 的两个根

$$x_1=\frac{1}{2}(3+\sqrt{-11}),\quad x_2=\frac{1}{2}(3-\sqrt{-11}).$$

全包含在 $K=\mathbf{Q}(\sqrt{-11})$ 中，$K/\mathbf{Q}$ 是一个单根式扩张，因而 $f(x)$ 的根不论按通常意义或按现在的定义都是可用根式解的．

例 2 §2 中的例 4, $f(x)=x^4+2x^2+2$ 它的四个根为 $\alpha,-\alpha,\beta,-\beta$ 而

$$\alpha=\sqrt{\sqrt{-1}-1},\quad \beta=\sqrt{-\sqrt{-1}-1},$$

且 $\alpha^2\beta^2=2$. 约定 $\alpha\cdot\beta=\sqrt{2}$. 于是 $\beta=\sqrt{2}\cdot\alpha^{-1}$. $f(x)$ 的分裂域 $E=\mathbf{Q}(\alpha,\beta)=\mathbf{Q}(\sqrt{-1},\sqrt{2},\alpha)$, 它本身就是一个根式扩张．因为 $E/\mathbf{Q}$ 有一个根式扩张链：

$$\mathbf{Q}\subset\mathbf{Q}(\sqrt{-1})=F_1\subset F_2=F_1(\sqrt{2})\subset F_3=F_2(\alpha)=E,$$

因而 $f(x)$ 的根在现在的意义下是可用根式解的．

一般说来，如果域 F 上一个多项式 $f(x)$ 的每个根都可以从 F 的元素出发经过有限步骤的五种运算 $+,-,\cdot,\div$ 及开任意次方而得到，那么，容易说明 $f(x)$

的全部根包含在比定义 6 弱一点的根式扩张链

$$F = L_0 \subset L_1 \subset \cdots \subset L_s = L \tag{2}$$

中，其中 $L_i = L_{i-1}(\theta_i)$，$\theta_i^{m_i} = b_{i-1} \in L_{i-1}$. 这里不要求 $m_i = [L_i : L_{i-1}]$，$i = 0, 1, \cdots, s-1$. 但是，下面将看到 $f(x)$ 的全部根可以包含在一个满足定义 6 的条件的根式扩张中. 反之，如果多项式 $f(x)$ 的全部根包含在根式扩张 K 中，而且 K 有一个根式扩张链 (1). 令 $F_i = F_{i-1}(\alpha_i), \alpha_i^{n_i} = \alpha_{i-1} \in F_{i-1}, n_i = [F_i : F_{i-1}]$. 那么 α_r 可表成 $\sqrt[n_r]{\alpha_{r-1}}$ 的形式，因而 K 的元素可以表成 $1, \sqrt[n_r]{\alpha_{r-1}}, \cdots, (\sqrt[n_r]{\alpha_{r-1}})^{n_r-1}$ 的线性组合，系数在 F_{r-1} 中. 对 r 作归纳法可知 K 的元素可以从 F 的元素出发经过有限次的 $+, -, \cdot, \div$ 和开方 (开 n_i 次方，$i = 1, \cdots, r$) 而得到. 因而 $f(x)$ 的每个根也如此，所以现在根式解的含义和通常的是相同的.

对于一个单根式扩张 $K = F(\alpha), \alpha^n = a \in F$，若次数 n 是一个复合数 $n = rs, r > 1, s > 1$，则在 F 与 K 之间插入中间域 $L = F(\alpha^r)$ 使得 $F \subset L \subset K$ 为一个根式扩张链，而且 $[L : F] = r, [K : L] = s$. 因此在定义 6 的 (1) 式中适当插入一些中间域可使 (1) 仍然保持是 K 的一个根式扩张链而且每个 $[F_i : F_{i-1}]$ 都是素数.

在伽罗瓦理论中，我们必须要求可以用根式解的这一类方程中自然要包括全部二项方程 $x^n - a$ $(a \in F)$ 在内，特别要包括 $x^n - 1$ 在内. 因此需要我们首先讨论 $x^n - 1$ 在 F 上的分裂域的伽罗瓦群.

定理 9 *$x^n - 1$ $(n > 0)$ 在有理数域 $\mathbf{Q}$ 上的分裂域 E 的伽罗瓦群和整数模 n 的环 $\mathbf{Z}/n\mathbf{Z}$ 的单位群 $\mathbf{Z}_n^* = (\mathbf{Z}/n\mathbf{Z})^*$ 同构.*

证明 由第七章 §6 知道，$x^n - 1$ 在 $\mathbf{Q}$ 上的分裂域可由任一个本原的 n 次单位根 ζ 生成，即 $E = \mathbf{Q}(\zeta)$. ζ 是分圆多项式 $\Phi_n(x)$ 的根. 由于 $\Phi_n(x)$ 是一个整系数多项式而且是不可约的，因而 $\Phi_n(x)$ 是 ζ 的极小多项式. 于是 E 对 $\mathbf{Q}$ 的次数等于 $\Phi_n(x)$ 的次数 $\varphi(n)$. 即 n 的欧拉函数值. 由定理 2 可知 $E/\mathbf{Q}$ 是一个伽罗瓦扩张，由定理 1 可知 $E/\mathbf{Q}$ 的伽罗瓦群 G 是一个 $\varphi(n)$ 阶群. 现决定 G. 根据 §1 引理 4,$\Phi_n(x)$ 的 $\varphi(n)$ 个根 ζ^ν, $(\nu, n) = 1$, 在 G 下是传递的. 对于每个 $\sigma \in G$, ζ 在 σ 下的象 $\sigma(\zeta)$ 是 $\Phi_n(x)$ 的一根，$\sigma(\zeta) = \zeta^\nu$. 反之，对 $\Phi_n(x)$ 每个根 ζ^ν, 有一个唯一的 $\sigma \in G$ 使得 $\sigma(\zeta) = \zeta^\nu$. 因此 G 的元素可记成 σ_ν, $(\nu, n) = 1$, 它由方程 $\sigma_\nu(\zeta) = \zeta^\nu$ 唯一决定. 显然 $\sigma_\nu = \sigma_\mu$ 当而且仅当 $\nu \equiv \mu \pmod n$, 由计算可知，$\sigma_\nu\sigma_\mu(\zeta) = \sigma_\nu(\zeta^\mu) = \zeta^{\nu\mu} = \sigma_{\nu\mu}(\zeta)$. 于是

$$\sigma_\nu \cdot \sigma_\mu = \sigma_{\nu\mu},$$

所以 $G \cong (\mathbf{Z}/n\mathbf{Z})^*$. □

定义 8 如果一个伽罗瓦扩张 E/F 的伽罗瓦群是一个交换群，则 E/F 叫做一个 **阿贝尔扩张**. 例如 $\mathbf{Q}$ 上的分圆域是一个阿贝尔扩张.

推论 设 F 为一个特征 0 的域， K 为 $x^n-1, n>0$, 在 F 上的分裂域. 则 $\mathrm{Gal}(K/F)$ 与 $(\mathbf{Z}/n\mathbf{Z})^*$ 的一个子群同构. 因而 K/F 是一个阿贝尔扩张.

证明 根据定理 3, $K=E\cdot F$ 复合域， $\mathrm{Gal}(K/F)\cong\mathrm{Gal}(E/E\cap F)$, 而后者是 $\mathrm{Gal}(E/\mathbf{Q})$ 的一个子群，因而它与 $(\mathbf{Z}/n\mathbf{Z})^*$ 的一个子群同构. □

定理 10 设 p 为一素数. 若域 F 包含 p 个不同的 p 次单位根，则 F 上任一个 p 次循环扩张 K 都是根式扩张.

证明 由假设， F 包含 p 个不同的 p 次单位根，那么 $x^p-1\in F[x]$ 是一个可分多项式. 它与微商 $(x^p-1)'=px^{p-1}$ 互素. 从而 $p\neq 0$. 由此可知 F 的特征或为 0 或者为一个素数. 若为后者，则 F 的特征必与 p 互素. 这 p 个 p 次单位根可由一个本原的 p 次单位根 ζ 生成： $1,\zeta,\zeta^2,\cdots,\zeta^{p-1}$. 其次，由题设 K/F 是 p 次循环扩张，则 $G=\mathrm{Gal}(K/F)$ 为一个 p 阶循环群，设由 σ 生成. 由于 $[K:F]=p$ 为素数， K 可由 F 外任一元素 θ 生成. 这是因为 $[F(\theta):F]>1$ 且整除 p, 必有 $[F(\theta):F]=p$, 从而 $F(\theta)=K$. 以下是证明的关键. 应用拉格朗日的预解式，就是利用 p 次单位根从 θ 作出一个新的生成元使得它的 p 次方属于 F. 令 $1,\zeta,\zeta^2,\cdots,\zeta^{p-1}$ 依次与 $\theta,\sigma(\theta),\sigma^2(\theta),\cdots,\sigma^{p-1}(\theta)$ 相乘后求和得

$$(\zeta,\theta)=\theta+\zeta\sigma(\theta)+\cdots+\zeta^{p-1}\sigma^{p-1}(\theta).$$

这个和数叫做 **拉格朗日预解式**. 它有如下的特性：用 σ 作用于 (ζ,θ), 注意 ζ 在 σ 下不动，

$$\sigma(\zeta,\theta)=\sigma(\theta)+\zeta\sigma^2(\theta)+\cdots+\zeta^{p-2}\sigma^{p-1}(\theta)+\zeta^{p-1}\theta=\zeta^{-1}(\zeta,\theta).$$

假若 $(\zeta,\theta)\neq 0$. 由于 $\zeta\neq 1$, 有 $\sigma(\zeta,\theta)\neq(\zeta,\theta)$, 由此可知 (ζ,θ) 不属于 F, 所以 (ζ,θ) 是 K 的一个生成元. 而且 (ζ,θ) 的 p 次方属于 F, 这是因为

$$\sigma((\zeta,\theta)^p)=(\sigma(\zeta,\theta))^p=(\zeta^{-1}(\zeta,\theta))^p=(\zeta,\theta)^p.$$

于是 $(\zeta,\theta)^p$ 是 σ 的也是 G 的一个不动元. 根据伽罗瓦扩张的定义， $(\zeta,\theta)^p$ 属于 F. 由此可知 K 是 F 上的一个根式扩张. 为了保证至少有一个拉格朗日预解式 (ζ,θ) 不等于 0. 我们联合考察 $p-1$ 个拉格朗日预解式 $(\zeta,\theta),(\zeta^2,\theta),\cdots,(\zeta^{p-1},\theta)$. 还加上一个 $(1,\theta)=\theta+\sigma(\theta)+\cdots+\sigma^{p-1}(\theta)$. 注意这个元素属于 F. 具体写出就是

$$\begin{aligned}(\zeta^\nu,\theta)&=\theta+\zeta^\nu\sigma(\theta)+\cdots+\zeta^{\nu(p-1)}\sigma^{p-1}(\theta),\\ \sigma(\zeta^\nu,\theta)&=\zeta^{-\nu}(\zeta^\nu,\theta);\quad \nu=0,1,\cdots,p-1.\end{aligned}\tag{3}$$

对 (3) 式两端求和, 注意 $\sigma^j(\theta)$ 的系数 $a_j = 1+\zeta^j+\zeta^{2j}+\cdots+\zeta^{(p-1)j}$ 当 $1 \le j < p$ 时, $a_j = 1+\zeta+\cdots+\zeta^{p-1} = 0$ 而 $a_0 = p$, 所以

$$(1,\theta)+(\zeta,\theta)+\cdots+(\zeta^{p-1},\theta) = p\theta.$$

由于 $\chi(F)=0$ 或 $(p,\chi(F))=1$, 因而 $p \neq 0$ 假设 $(\zeta,\theta),\cdots,(\zeta^{p-1},\theta)$ 全为 0, 则 $\theta = \dfrac{1}{p}(1,\theta) \in F$, 矛盾. 所以至少有一个 (ζ^ν,θ), $1 \le \nu < p$, 不等于 0, 这就完成了定理的证明. □

下面要用到可解群. 回忆一下有限可解群的一条基本性质: 一个有限可解群 G 有一个合成群列

$$G = G_0 \supset G_1 \supset \cdots \supset G_r$$

使得因子群 $G_i/G_{i+1}, i = 0,1,\cdots,r-1$ 都是素数阶循环群. 而且可解群的子群仍是可解群. (见第二章习题 42)

定理 11 (伽罗瓦) *设 F 为特征 0 的域, 若多项式 $f(x) \in F[x]$ 在 F 上的分裂域 E 的伽罗瓦群 $\mathrm{Gal}(E/F)$ 是可解的, 则 $f(x)$ 的根可用根式解.*

证明 我们证明与定理等价的命题: 若特征 0 的域 F 上有限伽罗瓦扩张 E 的伽罗瓦群 G 是可解的, 则 E 可以包含在一个根式扩张 K/F 中. 证明对次数 $[E:F]$ 作归纳法. 假设当 $[E:F] < n\ (n>1)$ 时命题成立, 求证当 $[E:F]=n$ 时命题也成立. 设 $p_1,\cdots,p_t$ 为 n 的全部相异的素因子, $m = p_1p_2\cdots p_t$, 设 ζ 为一个本原的 m 次单位根, 则 $F(\zeta)$ 是 F 上一个阿贝尔扩张, $[F(\zeta):F] \le \varphi(m) < n$. 阿贝尔群 $\mathrm{Gal}(F(\zeta)/F)$ 当然是可解群. 根据归纳法假设, $F(\zeta)$ 包含在一个根式扩张 L/F 中. 设

$$F = F_0 \subset F_1 \subset \cdots \subset F_s = L \tag{4}$$

是 L/F 的一个根式扩张链. 然后作 E 和 L 的复合域 $E\cdot L, H = \mathrm{Gal}(EL/L)$ 是 $G = \mathrm{Gal}(E/F)$ 的一个子群. 因为可解群的子群仍为一个可解群. 于是 H 有一个合成群列

$$H = H_0 \supset H_1 \supset \cdots \supset H_r$$

使得 H_i/H_{i-1} 是一个素数阶循环群, $i = 0,1,\cdots,r-1$ 在伽罗瓦对应下让 EL/L 的中间域 L_i/L 与子群 H_i 相对应. 于是得到 EL/L 的一个子域链

$$L = L_0 \subset L_1 \subset \cdots \subset L_r = EL, \tag{5}$$

使得 L_i 是 L_{i-1} 上伽罗瓦扩张, 而且 $\mathrm{Gal}(L_i/L_{i-1}) \cong H_i/H_{i-1}$. 因而 L_i/L_{i-1} 是素数次循环扩张, 而且 $[L_i:L_{i-1}]$ 都是 n 的素因子, 也是 m 的素因子. 由于 L 包含本原的 m 次单位根, 当然也包含每个本原 p_i 次单位根. 根据定理 10, 每

个 L_i/L_{i-1} 是一个单根式扩张. 将 (4) 和 (5) 连接起来就得到 EL/F 的一个根式扩张链. 于是 E 包含在根式扩张 EL/F 中. 这就完全证明了定理. □

下面着手证明定理 11 的逆定理. 首先证明定理 10 的逆定理.

定理 12 *设域 F 包含 n 个不同的 n 次单位根, $n>0$. 则二项式 $x^n-a, a\in F, a\neq 0$, 在 F 上的分裂域 E 的伽罗瓦群 G 为循环群, 其阶为 n 的因子. 特别, 若 x^n-a 在 F 上不可约, 则 $|G|=n$.*

证明 与定理 10 的开头一样, 由假设可知 F 的特征或为 0 或为一个素数而且它与 n 互素. F 的 n 个 n 次单位根可由一个本原的 n 次单位根 ζ 生成: $1,\zeta,\zeta^2,\cdots,\zeta^{n-1}$. 设 θ 为 x^n-a 的任一根, 则 x^n-a 的 n 个根为 $\theta,\zeta\theta,\zeta^2\theta,\cdots,\zeta^{n-1}\theta$. 它们全属于 $F(\theta)$, 因而 $E=F(\theta,\zeta\theta,\cdots,\zeta^{n-1}\theta)=F(\theta)$. 同样 $E=F(\zeta^i\theta)$, $i=0,1,\cdots,n-1$. 对于每个 $\sigma\in G, \sigma(\theta)$ 仍为 x^n-a 的一根, 设为 $\sigma(\theta)=\zeta^\nu\theta$. σ 由 θ 的象 $\zeta^\nu\theta$ 唯一决定, 因而 σ 可表成 σ_ν. 此时 σ_ν 和 σ_μ 相等当而且仅当 $\nu\equiv\mu \pmod n$. 由此建立了一个单一映射

$$\begin{gathered}G\to \mathbf{Z}/n\mathbf{Z}\\ \sigma_\nu\mapsto\overline{\nu}=\nu \pmod n,\end{gathered}$$

注意 $\sigma_\nu(\zeta)=\zeta$, 由计算

$$\begin{aligned}\sigma_\nu\sigma_\mu(\theta)&=\sigma_\nu(\sigma_\mu(\theta))=\sigma_\nu(\zeta^\mu\theta)=\zeta^\mu\sigma_\nu(\theta)\\&=\zeta^\mu\zeta^\nu\theta=\zeta^{\nu+\mu}\theta=\sigma_{\nu+\mu}(\theta),\end{aligned}$$

所以 $\sigma_\nu\cdot\sigma_\mu=\sigma_{\nu+\mu}$. 因而上述映射是一个单一同态. 所以 G 和加法群 $\mathbf{Z}/n\mathbf{Z}$ 的一个子群同构. 由于 $\mathbf{Z}/n\mathbf{Z}$ 是一个 n 阶循环加法群, 因而 G 是 n 阶循环群的一个子群, G 是一个循环群而且阶为 n 的因子. 若 x^n-a 在 F 上不可约, 则 $[E:F]=n$, 从而 $|G|=n$. 此时 G 是一个 n 阶循环群. □

推论 *设 p 为一素数而且 F 包含 p 个不同的 p 次单位根, 则二项式 $x^p-a, a\in F, a\neq 0$, 在 F 上分裂域 E 或是一个 p 次循环扩张或者 $E=F$ 按照 a 在 F 内不能开 p 次方或否而定.*

证明 根据定理 12,E/F 的伽罗瓦群只能是 p 阶群或单位元群, 因而 E/F 只能是 p 次扩张或 $E=F$. 若 $E=F$, 则 x^p-a 在 F 完全分解成一次因式之积, 即 $\theta,\zeta\theta,\cdots,\zeta^{p-1}\theta$ 全属于 F. 此时 $-a=(-1)^p\theta\cdot\zeta\theta\cdots\zeta^{p-1}\theta=(-1)^p\cdot(-1)^{p-1}\theta^p$, 即 $a=\theta^p$, a 在 F 内可开 p 次方. 反之, 设 a 在 F 内可开 p 次方, $\theta\in F$ 为 a 的一个 p 次根. 于是 $x^p-a=x^p-\theta^p=(x-\theta)(x-\zeta\theta)\cdots(x-\zeta^{p-1}\theta)$, $x-\zeta^\nu\theta\in F[x]$, 所以 $E=F(\theta,\zeta\theta,\cdots,\zeta^{p-1}\theta)=F$. 总之, $E=F$ 当而且仅当 a 在 F 内可开 p 次方. □

引理　设 K/F 为一根式扩张，$F=F_0\subset F_1\subset\cdots\subset F_t=K$ 为它的一个根式扩张链，并假定当 $\chi(F)$ 为素数时所有 $[F_i:F_{i-1}]$ 都与 $\chi(F)$ 互素．则 K/F 的正规闭包 E/F 的伽罗瓦群 G 是可解的．而且 $|G|$ 的素因子不超出所有 $[F_i:F_{i-1}]$ 所含的素因子．

证明　首先由假设可知 K/F 是可分的，因而 E/F 也可分，它是伽罗瓦扩张．设 $F_i=F_{i-1}(\alpha_i),\alpha_i^{p_i}=a_{i-1}\in F_{i-1},p_i=[F_i:F_{i-1}]$ 而且不妨设 $p_i\ (i=1,\cdots,t)$ 都是素数．E 在 F 上正规，当然 E 在每个 F_{i-1} 上也正规．$x^{p_i}-a_{i-1}$ 是 F_{i-1} 上不可约多项式且在 E 内有一根 α_i，而且当 $\chi(F)$ 为素数时，p_i 与 $\chi(F)$ 互素，因此 $x^{p_i}-a_{i-1}$ 在 F_{i-1} 上可分，它的 p_i 个根 $\alpha_i,\zeta_i\alpha_i,\cdots,\zeta_i^{p_i-1}\alpha_i$ 全在 E 内，其中 ζ_i 为一个本原的 p_i 次单位根．于是 $\zeta_i=\zeta_i\alpha_i/\alpha_i$，$i=1,\cdots,t$，全属于 E．令 $K_0=F(\zeta_1,\cdots,\zeta_t)$．根据定理 9 的推论以及 §3 的最后的说明，$K_0$ 是 F 上的阿贝尔扩张．显然 K_0 包含全部本原的 p_i 次单位根 ζ_i．其次，在 K_0 上作出一个根式扩张链．首先将 G 作用于 α_1 得到一个传递集 $\alpha_1,\sigma_2(\alpha_1),\cdots,\sigma_{r_1}(\alpha_1)$．令 $K_1=K_0(\alpha_1,\sigma_2(\alpha_1),\cdots,\sigma_{r_1}(\alpha_1))$．显然 K_1 在 G 下是稳定的．就是说，对所有 $\sigma\in G$ 有 $\sigma(K_1)\subset K_1$．因此 K_1 在 F 上正规．从 K_0 到 K_1 有一个扩张链

$$K_0\subset K_0(\alpha_1)\subset K_0(\alpha_1,\sigma_2(\alpha_1))\subset\cdots\subset K_0(\alpha_1,\sigma_2(\alpha_1),\cdots,\sigma_{r_1}(\alpha_1))=K_1.\quad(6)$$

由于 $\sigma_i(\alpha_1)^{p_1}=\sigma_i(\alpha_1^{p_1})=\sigma_i(a_0)=a_0\in F$，当然 $\sigma_i(\alpha_1)^{p_1}=a_0\in K_0$．因而 (6) 是 K_1/K_0 的一个根式扩张链，后一项是前一项的一个 p_1 次根式扩张即 p_1 次循环扩张或等于前一项 (定理 12 及其推论)．其次将 G 作用于 α_2 得到一个传递集 $\alpha_2,\tau_2(\alpha_2),\cdots,\tau_{r_2}(\alpha_2)$．令 $K_2=K_1(\alpha_2,\tau_2(\alpha_2),\cdots,\tau_{r_2}(\alpha_2))$．同理可知 K_2 在 F 上正规而且从 K_1 到 K_2 有一个根式扩张链

$$K_1\subset K_1(\alpha_2)\subset K_1(\alpha_2,\tau_2(\alpha_2))\subset\cdots\subset K_1(\alpha_2,\cdots,\tau_{r_2}(\alpha_2))=K_2.$$

其中后一项是前一项的一个 p_2 次根扩张即 p_2 次循环扩张或者等于前一项．这样继续下去，我们作出一个扩张链

$$F\subset K_0\subset K_1\subset\cdots\subset K_t,$$

使得 K_i 都是 F 上正规扩张，从 K_i 到 K_{i+1} 有一个根式扩张链使得后一项是前一项的 p_{i+1} 次循环扩张，而且 K_t 包含 $\alpha_1,\alpha_2,\cdots,\alpha_t$，因而 K_t 包含 K．由于 E 是 K 在 F 上的正规闭包，必然 $K_t=E$．在伽罗瓦对应下令 G 的子群 G_i 与 K_i 相对应，于是 G_i 都是 G 的正规子群．而且根据上面的作法，可知从 G_i 到 G_{i+1} 有一个子群列

$$G_i=G_{i0}\supset G_{i1}\supset\cdots\supset G_{is_i}=G_{i+1},\quad i=0,\cdots,t-1.$$

使得 $G_{ij+1} \lhd G_{ij}$ 而且商群 G_{ij}/G_{ij+1} 是一个素数 p_{i+1} 阶循环群. 加之, $G/G_0 = \mathrm{Gal}(K_0/F)$ 是一个阿贝尔群, 所以 G 是一个可解群. □

我们知道, 可解群的同态象还是一个可解群. (见第二章习题 42.)

定理 13 (伽罗瓦) *设 $\chi(F) = 0, E/F$ 为 F 上一个多项式 $f(x)$ 的分裂域, 若 $f(x)$ 可用根式解, 则 E/F 的伽罗瓦群是可解的.*

证明 根据根式解的定义, $f(x)$ 的分裂域 E 包含在一个根式扩张 K/F 中. 由引理可知, K/F 的正规闭包 $\overline{E}/F$ 是伽罗瓦扩张而且 $\mathrm{Gal}(\overline{E}/F) = \overline{G}$ 是一个可解群. 在伽罗瓦对应下设 E 与 $\overline{G}$ 的子群 H 对应, 则 H 在 $\overline{G}$ 内正规而且 $\mathrm{Gal}(E/F) \cong \overline{G}/H$. 因为可解群的商群仍为可解群, $\overline{G}/H$ 可解. 所以 $\mathrm{Gal}(E/F)$ 可解. □

综合定理 11 和定理 13, 我们得到

方程的根可用根式解的判别准则 *在特征 0 的域 F 上, 多项式 $f(x)$ 的根可用根式解的充分必要条件是 $f(x)$ 的分裂域 E/F 的伽罗瓦群是可解的.*

定理 11 的一个特殊情况是: $x^n - 1$ 在特征 0 的域上是可以用根式解的. 当 n 为素数时, 在伽罗瓦之前已为高斯所证明. 反过来, 这个特殊情况又是定理 11 成立的前提. 定理 11 可以推广成

定理 11′ *设 E/F 为域 F 上一个可分多项式 $f(x)$ 的分裂域. 当 $\chi(F)$ 为素数时, 还假定次数 $[E:F]$ 的每个素因子小于 $\chi(F)$. 于是, 若 $\mathrm{Gal}(E/F)$ 可解, 则 $f(x)$ 可用根式解.*

定理 11 的证明完全可以照搬过来作为定理 11′ 的证明. 只要注意在那里的次数 $[F(\zeta):F]$ 不仅小于 n 而且它的每个素因子也是 $\varphi(m)$ 的素因子, 因而小于 $\chi(F)$(当 $\chi(F)$ 为素数时). □

定理 13 也可以推广成

定理 13′ *设域 F 上一个可分多项式的分裂域 E/F 包含在一个根式扩张链*

$$F = F_0 \subset F_1 \subset \cdots \subset F_r = K$$

中, 而且假定当 $\chi(F)$ 为素数时, 每个 $[F_i : F_{i-1}]$ 与 $\chi(F)$ 互素. 于是 $\mathrm{Gal}(E/F)$ 是可解的.

定理 13 的证明完全适用定理 13′. □

说明. 从定理 11′ 和定理 13′ 看到, 当基域 F 的特征为素数 p 时, F 上可分多项式 $f(x)$ 可用根式解的充分条件比它的必要条件要强一些. 这一点可参看本章习题 46.

§5 n 次一般方程的群

我们说域 F 上 n 次一般方程是指下列方程

$$f(x) = x^n + t_1 x^{n-1} + \cdots + t_n = 0,$$

其中 $t_1, \cdots, t_n$ 是 F 上的独立未定元即代数无关元. 实际上, $f(x)$ 并不是 F 上的多项式而是 n 元多项式环 $R = F[t_1, \cdots, t_n]$ 上的多项式. 问题是确定 $f(x)$ 在 R 的商域 $F(t_1, \cdots, t_n)$ 上的伽罗瓦群. 如果这群是可解的, 并假定当 $\chi(F)$ 为素数时, $\chi(F)$ 大于 n 的每个素因子, 则可进而导出 $f(x)$ 的根用根式解的表达式. 从此得到如下的结论: F 上任意 n 次可分多项式 $g(x) = x^n + a_1 x^{n-1} + \cdots + a_n, a_i \in F$, 在 F 上可用根式解, 而且它的解可在上述表达式中用 a_i 代入 t_i 而得到. 这就是所谓的公式解. 为了决定 $f(x)$ 的群, 先考虑 F 上 n 次多项式环 $F[x_1, \cdots, x_n]$ 的一个 F- 自同构群. 设 S_n 为文字 $1, 2, \cdots, n$ 的对称群, 每个 $\sigma \in S_n$ 引起 $F[x_1, \cdots, x_n]$ 的一个自同构

$$\psi(x_1, \cdots, x_n) \mapsto \psi(x_{\sigma(1)}, \cdots, x_{\sigma(n)}),$$

而且它还保持 F 的元素不动. 这个 F- 自同构由 $x_1, \cdots, x_n$ 的象 $x_{\sigma(1)}, \cdots, x_{\sigma(n)}$ 唯一决定, 仍记作 σ. 这个自同构还可唯一地开拓成 $F[x_1, \cdots, x_n]$ 的商域 $K = F(x_1, \cdots, x_n)$ 的 F- 自同构 $\overline{\sigma}$, 对于 $\varphi(x_1, \cdots, x_n), \psi(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$, 规定

$$\overline{\sigma}\left(\frac{\varphi(x_1, \cdots, x_n)}{\psi(x_1, \cdots, x_n)}\right) = \frac{\sigma\varphi(x_1, \cdots, x_n)}{\sigma\psi(x_1, \cdots, x_n)},$$

不难验证, 对于 $\sigma, \tau \in S_n$, 有 $\overline{\sigma} \cdot \overline{\tau} = \overline{\sigma\tau}$, 而且当 $\sigma \neq \tau$ 时, 显然 $\overline{\sigma} \neq \overline{\tau}$. 这样得到 K 的一个 F- 自同构群, 与 S_n 同构. 为简单起见, 让 $\overline{\sigma}$ 仍记为 σ, S_n 看作 K 的 F- 自同构群. 用 F_1 表示 S_n 的不动域, 根据定理 1, $[K : F_1] = |S_n| = n!$. 显然 $F \subset F_1$ 而且 F_1 还包含 $x_1, \cdots, x_n$ 的初等对称函数

$$\sigma_1 = x_1 + x_2 + \cdots + x_n,$$
$$\sigma_2 = x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\sigma_n = x_1 x_2 \cdots x_n.$$

因而 $F(\sigma_1, \cdots, \sigma_n) \subset F_1$, 从而 $[K : F(\sigma_1, \cdots, \sigma_n)] \geq [K : F_1] = n!$. 另一方面, $g(x) = (x - x_1)(x - x_2) \cdots (x - x_n) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n$ 是 $F(\sigma_1, \cdots, \sigma_n)$ 上的多项式, 它在 $F(\sigma_1, \cdots, \sigma_n)$ 上的分裂域为 $F(\sigma_1, \cdots, \sigma_n)(x_1, \cdots, x_n) = F(x_1, \cdots, x_n) = K$. 因而次数 $[K : F(\sigma_1, \cdots, \sigma_n)] \leq n!$(参看第七章定理 5 的

推论). 总之 $[K:F_1]=[K:F(\sigma_1,\cdots,\sigma_n)]=n!$, 由 $F(\sigma_1,\cdots,\sigma_n)\subset F_1$ 可知 $F(\sigma_1,\cdots,\sigma_n)=F_1$. 因而 K 是 $F(\sigma_1,\cdots,\sigma_n)$ 上的伽罗瓦扩张而且它的群为 n 个文字的对称群 S_n.

设 E 为 F 上 n 次一般方程 $f(x)=x^n+t_1x^{n-1}+\cdots+t_n$ 的分裂域 (在 $F(t_1,\cdots,t_n)$ 上),$u_1,\cdots,u_n$ 表示 $f(x)$ 的根. 于是 $E=F(t_1,\cdots,t_n)(u_1,\cdots,u_n)=$

$F(u_1,\cdots,u_n)$. E 包含一个子环 $F[u_1,\cdots,u_n]$, 它是 F 上一个有限生成的环. 我们可以应用第三章定理 15. 来建立环同态 $\eta:F[x_1,\cdots,x_n]\to F[u_1,\cdots,u_n]$ 使得 $\eta(x_i)=u_i$ 而且 η 限制在 F 上为恒等同构. η 是满的. 而且 η 作用在 $x_1,\cdots,x_n$ 的初等对称函数 σ_i 上有

$$\eta(\sigma_i)=\eta\left(\sum_{\nu_1<\cdots<\nu_i}x_{\nu_1}x_{\nu_2}\cdots x_{\nu_i}\right)=\sum_{\nu_1<\cdots<\nu_i}u_{\nu_1}u_{\nu_2}\cdots u_{\nu_i}=(-1)^it_i.$$

$t_1,\cdots,t_n$ 在 F 上代数无关, 从而推出它们的原象 $-\sigma_1,\sigma_2,\cdots,(-1)^n\sigma_n$ 在 F 上也代数无关. 我们进一步证明 η 是单一的. 设 η 将一个 $g(x_1,\cdots,x_n)$ 变成 0, 作

$$\psi(x_1,\cdots,x_n)=\prod_{\pi\in S_n}\pi(g(x_1,\cdots,x_n)),$$

于是 $\pi(\psi(x_1,\cdots,x_n))=\psi(x_1,\cdots,x_n)$ 对所有的 $\pi\in S_n$. 于是 $\psi(x_1,\cdots,x_n)$ 属于 S_n 的不动域 $F(\sigma_1,\cdots,\sigma_n)$. 加之, $\psi(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$, 因而 $\psi(x_1,\cdots,x_n)$ 可唯一地表成 $\sigma_1,\cdots,\sigma_n$ 的多项式, 设 $\psi(x_1,\cdots,x_n)=\varphi(\sigma_1,\cdots,\sigma_n)\in F[\sigma_1,\cdots,\sigma_n]$. 一方面 $\eta(\varphi(\sigma_1,\cdots,\sigma_n))=\eta(\psi(x_1,\cdots,x_n))=\prod_{\pi\in S_n}\eta(\pi(g(x_1,\cdots,x_n)))=0$. 另一方面, $\eta(\varphi(\sigma_1,\cdots,\sigma_n))=\varphi(-t_1,\cdots,(-1)^nt_n)$, 从而 $\varphi(-t_1,\cdots,(-1)^nt_n)=0$. 由于 $t_1,\cdots,t_n$ 在 F 上代数无关, 可知 $\varphi(-t_1,\cdots,(-1)^nt_n)$ 中 $t_1,\cdots,t_n$ 的每个单项式的系数为 0, 从而推出 $\varphi(\sigma_1,\cdots,\sigma_n)$ 中 $\sigma_1,\cdots,\sigma_n$ 的每个单项式的系数也为 0. 由此推出 $\psi(x_1,\cdots,x_n)=0$, $g(x_1,\cdots,x_n)=0$. 因而 η 是单射的. 于是 $F[x_1,\cdots,x_n]\cong F[u_1,\cdots,u_n]$. 由此可知它们的商域 $F(x_1,\cdots,x_n)\cong F(u_1,\cdots,u_n)$, 即 $K\cong E$ 而且 σ 诱导出 $F(\sigma_1,\cdots,\sigma_n)\cong F(t_1,\cdots,t_n)$. 所以 E 在 $F(t_1,\cdots,t_n)$ 上的伽罗瓦群同构于 K 在 $F(\sigma_1,\cdots,\sigma_n)$ 上的伽罗瓦群即 S_n. 于是得

定理 14 *域 F 上 n 次一般方程 $f(x)=x^n+t_1x^{n-1}+\cdots+t_n$ 在 $F(t_1,\cdots,t_n)$ 上是可分的. $f(x)$ 在 $F(t_1,\cdots,t_n)$ 上的伽罗瓦群是 n 个文字的对称群.*

我们知道, 当 $n\le 4$ 时对称群 S_n 是可解的, 而当 $n\ge 5$ 时 S_n 是不可解的. 于是得

定理 15 (阿贝尔 - 鲁菲尼) $n \geq 5$ 的一般方程 $f(x) = x^n + t_1 x^{n-1} + \cdots + t_n$ 在 $F(t_1, \cdots, t_n)$ 上是不能用根式解的.

以下讨论域 F 上三次和四次一般方程的根式解.

例 1 $f(x) = x^3 + t_1 x^2 + t_2 x + t_3, \chi(F) \neq 2, 3$.

解 因 $\chi(F) \neq 3$, 作替换 $x = y - \frac{t_1}{3}$, $f\left(y - \frac{t_1}{3}\right) = g(y) = y^3 + py + q$, $p = -\frac{t_1^2}{3} + t_2, q = \frac{1}{27}(2t_1^3 - 9t_1t_2 + 27t_3)$. p 和 q 在 F 上代数无关. 令 $F_1 = F(t_1, t_2, t_3)$. $g(y)$ 和 $f(x)$ 有相同的分裂域 E/F_1, 因而它们的群同构. 仍用 S_3 表示 $g(y)$ 的群, $\beta_1, \beta_2, \beta_3$ 表示 $g(y)$ 的根. $S_3 = \langle \sigma, \tau \rangle, \sigma = (123), \tau = (12)$. $g(y)$ 的判别式 $D = -4p^3 - 27q^2$. 由于 $\chi(F) \neq 2$, 根据定理 5, 与 $F_2 = F_1(\sqrt{D})$ 对应的 S_3 的子群是 $A_3 = \langle \sigma \rangle, \mathrm{Gal}(E/F_2) = A_3$. 因而 E/F_2 是一个 3 次循环扩张. 由定理 10 知道, 求解 3 次循环扩张, 需要添加 3 次单位根到基域 F_2. 由于 $\chi(F) \neq 2, 3$, 本原的 3 次单位根 ω 可以用根式表出 $\omega = \frac{1}{2}(-1 + \sqrt{-3})$, 另一根为 ω^2. 将 ω 添加到 F_2, 于是 $E(\omega)$ 仍是 $F_2(\omega)$ 上的 3 次循环扩张, 而且 $E(\omega) = F_2(\beta_1, \beta_2, \beta_3)(\omega) = F_2(\omega)(\beta_1, \beta_2, \beta_3) = F_2(\omega)(\beta_1)$. 于是应用定理 10, 作拉格朗日预解式

$$\begin{aligned}
(\omega, \beta_1) &= \beta_1 + \omega\sigma(\beta_1) + \omega^2\sigma^2(\beta_1) = \beta_1 + \omega\beta_2 + \omega^2\beta_3, \\
(\omega^2, \beta_1) &= \beta_1 + \omega^2\sigma(\beta_1) + \omega\sigma^2(\beta_1) = \beta_1 + \omega^2\beta_2 + \omega\beta_3, \\
(1, \beta_1) &= \beta_1 + \sigma(\beta_1) + \sigma^2(\beta_1) = \beta_1 + \beta_2 + \beta_3 = 0.
\end{aligned}$$

已知 $(\omega, \beta_1)^3, (\omega^2, \beta_1)^3 \in F_2(\omega)$. 应用恒等式 $X^3 + Y^3 = (X + Y)(X + \omega Y)(X + \omega^2 Y)$, 计算

$$\begin{aligned}
(\omega, \beta_1)^3 + (\omega^2, \beta_1)^3 &= 3\beta_1 \cdot 3\omega^2\beta_3 \cdot 3\omega\beta_2 = 27(-q) = -27q. \\
(\omega, \beta_1)^3 \cdot (\omega^2, \beta_1)^3 &= [(\omega, \beta_1)(\omega^2, \beta_1)]^3 = [\beta_1^2 + \beta_2^2 + \beta_3^2 - \beta_1\beta_2 - \beta_2\beta_3 - \beta_3\beta_1]^3 \\
&= (-3p)^3.
\end{aligned}$$

因而 $(\omega, \beta_1)^3$ 和 $(\omega^2, \beta_1)^3$ 适合二次方程 $x^2 + 27qx - (3p)^3$. 所以

$$\begin{aligned}
(\omega, \beta_1)^3 &= -\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}, \\
(\omega^2, \beta_1)^3 &= -\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}.
\end{aligned} \tag{1}$$

(ω, β_1) 和 (ω^2, β_1) 分别是上两式右端的立方根, 各有三个值, 可以配成九对, 但是 (ω, β_1) 的值和 (ω^2, β_1) 的值配成的对必须满足代数关系

$$(\omega, \beta_1) \cdot (\omega^2, \beta_1) = -3p.$$

满足这种关系的只有三对值，任取其中一对，代入下式

$$\begin{aligned}\beta_1 &= \frac{1}{3}((\omega,\beta_1)+(\omega^2,\beta_1)),\\ \beta_2 &= \frac{1}{3}(\omega^{-1}(\omega,\beta_1)+\omega^{-2}(\omega^2,\beta_1)),\\ \beta_2 &= \frac{1}{3}(\omega^{-2}(\omega,\beta_1)+\omega^{-2}(\omega^2,\beta_1)),\end{aligned} \tag{2}$$

就得到 $g(y)$ 的三个根. 若取其它两对代入上式得到的三根只差一个轮换. 最后得到 $f(x)$ 的三根 $\alpha_i=\beta_i-\dfrac{t_1}{3}$, $i=1,2,3$. (1) 和 (2) 就是 3 次方程的公式解. 当然一些特殊的 3 次方程有其特殊的解法, 不必套用公式. 套用公式反而使计算复杂.

例 2 $f(x)=x^4+t_1x^3+t_2x^2+t_3x+t_4$, $\chi(F)\neq 2,3$.

解 因 $\chi(F)\neq 2$, 作替换 $x=y-\dfrac{t_1}{4}$ 代入 $f(x)$, 得 $f\left(y-\dfrac{t_1}{4}\right)=g(y)=y^4+py^2+qy+r$, 其中 $p=-\dfrac{3}{8}t_1^2+t_2$, $q=\dfrac{1}{8}t_1^3-\dfrac{1}{2}t_1t_2+t_3$, $r=-\dfrac{3}{256}t_1^4+\dfrac{1}{16}t_1^2t_2-\dfrac{1}{4}t_1t_3+t_4$. 令 $F_1=F(t_1,\cdots,t_4)$. $f(x)$ 和 $g(y)$ 在 F_1 上有相同的分裂域 E, 因而 $g(y)$ 在 F_1 上的群仍为 S_4. $g(y)$ 的根记作 $\beta_1,\beta_2,\beta_3,\beta_4$. S_4 中 4 阶正规子群 V 由 $\sigma=(12)(34)$, $\tau=(13)(24)$ 生成. 在伽罗瓦对应下与子群 V 对应的 E/F_1 的中间域, 根据定理 6, 是 F_1 上 6 次扩张, 它由

$$\theta_1=(\beta_1+\beta_2)(\beta_3+\beta_4),\theta_2=(\beta_2+\beta_3)(\beta_1+\beta_4),\theta_3=(\beta_1+\beta_3)(\beta_2+\beta_4)$$

生成, 记成 $K=F_1(\theta_1,\theta_2,\theta_3)$. θ_i 所适合的 3 次多项式为 $h(x)=x^3+b_1x^2+b_2x+b_3$, 其中 $b_1=-2p$, $b_2=p^2-4r$, $b_3=q^2$. $h(x)$ 就是 $f(x)$ 的 3 次预解式. 以上的讨论在假定 $\chi(F)\neq 2$ 下都有效. 为了能用根式求解 $h(x)$ 的根, 还需假定 $\chi(F)\neq 2,3$. 这时可应用例 1 得到的 $h(x)$ 的根式解, 即将 $\theta_1,\theta_2,\theta_3$ 用根式表出. 假设 $\theta_1,\theta_2,\theta_3$ 已经用根式表出. 下面的问题是如何将 $g(y)$ 的根用 θ_i 和它们的根式表出. E/K 的伽罗瓦群是 V. 在 E 中取一个根的函数, 它在 V 下是二值的, 例如 $\beta_1+\beta_2$ 就是这样的函数: $\sigma(\beta_1+\beta_2)=\beta_1+\beta_2$, $\tau(\beta_1+\beta_2)=\beta_3+\beta_4$, $\sigma\tau(\beta_1+\beta_2)=\beta_4+\beta_3$. $\beta_1+\beta_2$ 在 V 下只有两个值 $\beta_1+\beta_2$ 和 $\beta_3+\beta_4$. 它们适合方程

$$x^2+\theta_1=0\ \ (\text{因}\beta_1+\beta_2+\beta_3+\beta_4=0)$$

解出 $\beta_1+\beta_2=\sqrt{-\theta_1}$, $\beta_3+\beta_4=-\sqrt{-\theta_1}$. 同理得

$$\begin{aligned}\beta_2+\beta_3=\sqrt{-\theta_2},\quad \beta_1+\beta_4=-\sqrt{-\theta_2},\\ \beta_1+\beta_3=\sqrt{-\theta_3},\quad \beta_2+\beta_4=-\sqrt{-\theta_3}.\end{aligned} \tag{3}$$

$\sqrt{-\theta_1},\sqrt{-\theta_2}$ 和 $\sqrt{-\theta_3}$ 各有两个值，如何匹配才能得到正确的 $\beta_i+\beta_j$ $(i\neq j)$ 的值，这需要考察 $\beta_1+\beta_2,\beta_2+\beta_3,\beta_1+\beta_3$ 在 K 上的代数关系．由计算

$$\begin{aligned}&(\beta_1+\beta_2)(\beta_2+\beta_3)(\beta_1+\beta_3)\\&\quad=-(\beta_1+\beta_2)(\beta_1+\beta_4)(\beta_1+\beta_3)\\&\quad=-[\beta_1^3+\beta_1^2(\beta_2+\beta_3+\beta_4)+\beta_1(\beta_2\beta_3+\beta_2\beta_4+\beta_3\beta_4)+\beta_2\beta_3\beta_4],\end{aligned}$$

注意

$$\begin{aligned}&\beta_2+\beta_3+\beta_4=-\beta_1,\\&\beta_1\beta_2\beta_3+\beta_1\beta_2\beta_4+\beta_1\beta_3\beta_4+\beta_2\beta_3\beta_4=-q.\end{aligned}$$

所以 $\sqrt{-\theta_1},\sqrt{-\theta_2},\sqrt{-\theta_3}$ 的取值应满足

$$\sqrt{-\theta_1}\cdot\sqrt{-\theta_2}\cdot\sqrt{-\theta_3}=q.$$

然后从 (3) 解出 $\beta_1,\beta_2,\beta_3,\beta_4$ 如下

$$\begin{aligned}\beta_1&=\frac{1}{2}(\sqrt{-\theta_1}-\sqrt{-\theta_2}+\sqrt{-\theta_3}),\\\beta_2&=\frac{1}{2}(\sqrt{-\theta_1}+\sqrt{-\theta_2}-\sqrt{-\theta_3}),\\\beta_3&=\frac{1}{2}(-\sqrt{-\theta_1}+\sqrt{-\theta_2}+\sqrt{-\theta_3}),\\\beta_4&=\frac{1}{2}(-\sqrt{-\theta_1}-\sqrt{-\theta_2}-\sqrt{-\theta_3}).\end{aligned}$$

代回即得 $f(x)$ 的四个根 $\alpha_i=\beta_i-\dfrac{t_1}{4}$, $i=1,2,3,4$.

§6 尺规作图

尺规作图是初等平面几何的基本问题之一．简单地说，就是在欧几里得平面上，应用无刻度的直尺和圆规从已知的图形 (如点、直线和圆等) 出发作出未知的图形．本节的目的是研究什么样的几何图形可以用尺规作出．

初等平面几何中作图问题，如求作过一已知点并和一已知直线平行 (或垂直) 的直线；将一已知线段 n 等分；作一已知角的分角线；求作一已知三角形的内切圆等等问题．都可以叙述成如下的一般性的作图问题：

定义 9 在欧几里得平面上任给一个有限点集 $S_0=\{P_1,P_2,\cdots,P_n\}$, $n\geq 2$, 我们只允许用无刻度的直尺和圆规作如下的图形

1) 过 S_0 的任两点作直线．

2) 以 S_0 的任一点为圆心，以 S_0 的任两点的距离为半径作圆．

如果平面上一点 P 是 1) 中两直线的交点或是 1) 中一直线和 2) 中一圆的交点

或是 2) 中两圆的交点，则称点 P**可用尺规直接从** S_0 **作出**. 如果对点 P 存在一串点 $P_1',\cdots,P_r',P_r'=P$ 使得 P_1' 可用尺规直接从 S_0 作出而且 P_{i+1}' 可用尺规直接从点集 $S_0\cup\{P_1',\cdots,P_i'\}$ 作出，则称 P**可用尺规从** S_0 **作出**.

为了给出点 P 可作的条件，我们引进平面的直角坐标系，取 P_1P_2 分别作为坐标原点 O 和 x- 轴上单位点 E. 这样就建立了平面直角坐标系，从而赋予了每点 P_i 以坐标 (a_i,b_i), 特别 $P_1=(0,0),P_2=(1,0)$. 这样，单从原点 O 和单位点 E 出发能作出哪些点？首先在 x- 轴上可作出坐标为整数的点 $(r,0),r\in\mathbf{Z}$. 然后作过 O 点且与 x- 轴垂直的直线即 y- 轴. 在 y- 轴上可作出一切点 $(0,s),s\in\mathbf{Z}$. 进而作出平面上一切格点 $(r,s),r,s\in\mathbf{Z}$. 再作线段 $\overline{OQ},Q=(r,s)$ 的 m 分点 $\left(\frac{r}{m},\frac{s}{m}\right)$. 这样就作出了平面上的一切有理点. 这个点集在平面上稠密. 当然还可作出更多的点.

注意. 若点 $P(a,b)$ 可以用尺规从 S_0 作出，则 P 至 x- 轴和 y- 轴的垂足 $(a,0)$ 和 $(0,b)$ 也可用尺规从 S_0 作出. 而且与 P 成 x- 轴对称的点 $(a,-b)$ 以及绕原点反时针方向旋转 $\frac{\pi}{2}$ 得到 P 的象点 $(-b,a)$ 都可以从 S_0 作出.

为了以后的应用，我们把平面上的点用复数表示. 在给定的直角坐标系中将点 $P(a,b)$ 看作复数 $z=a+b\sqrt{-1}$. 以后点 $P(a,b)$ 和复数 $z=a+b\sqrt{-1}$ 可以互相表示. 于是上述基本事实又可表成：

域 $\mathbf{Q}(\sqrt{-1})$ 的每个数都可以用尺规从数集 $\{0,1\}$ 作出.

这样对数集 $\{0,1\}$ 引进了基域 $\mathbf{Q}(\sqrt{-1})$, 对任意给定的复数 $z_1,\cdots,z_n\ (n\geq 0)$, 由上面的注意可知，若复数 $z=a+b\sqrt{-1}$ 可用尺规从 $S_0=\{0,1,z_1,\cdots,z_n\}$ 作出，那么 a 和 b 也可用尺规从 S_0 作出. 因此对 S_0 也引进一个基域 $F_1=\mathbf{Q}(\sqrt{-1},z_1,\cdots,z_n,\overline{z}_1,\cdots,\overline{z}_n)$, $\overline{z}_i$ 为 z_i 的共轭. 设 $z_i=a_i+b_i\sqrt{-1},i=1,\cdots,n$, 则 $\overline{z}_i=a_i-b_i\sqrt{-1}$. 而且 F_1 包含 $a_i=\frac{1}{2}(z_i+\overline{z}_i)$ 和 $b_i=-\frac{1}{2}(z_i-\overline{z}_i)\sqrt{-1}$. 因而 F_1 包含一个实子域 $F_0=\mathbf{Q}(a_1,\cdots,a_n,b_1,\cdots,b_n)$ 而且

$$F_1=F_0(\sqrt{-1}).$$

定理 16 *任给复数 $z_i=a_i+b_i\sqrt{-1},\ i=1,\cdots,n,\ n\geq 0$, 并设 $F_1=\mathbf{Q}(\sqrt{-1},z_1,\cdots,z_n,\overline{z}_1,\cdots,\overline{z}_n)$. 于是复数 z 可以用尺规从数集 $S_0=\{0,1,z_1,\cdots,z_n\}$ 作出的充要条件是存在一个根式扩张 K/F_1, 使得*

1) $z\in K$;

2) *K/F_1 有一个二次根式扩张链*

$$F_1\subset F_2\subset\cdots\subset F_r=K,\ [F_{i+1}:F_i]=2,\ i=1,\cdots,r-1. \tag{1}$$

证明 必要性. 设复数 $z=\alpha+\beta\sqrt{-1}$ 可用尺规直接从 S_0 作出. 于是有三种情况:

i) z 是两直线

$$ax+by+c=0, \tag{2}$$

$$a'x+b'y+c'=0 \tag{3}$$

的交点, 而 (2) 和 (3) 分别是过 S_0 中两对点的直线. 由解析几何知道, 系数 a,b,c 和 a',b',c' 分别是该两对点的坐标的有理分式, 因而都属于 F_0. 应用克拉默法则解出 z, 可知 α 和 β 都是这六个系数的有理分式, 因而 α,β 都属于 F_0. 从而 $z\in F_1$.

ii) z 是直线 (2) 和圆

$$x^2+y^2+dx+ey+f=0 \tag{4}$$

的交点, 而 (4) 是以 S_0 中一点为圆心以其中两点的距离为半径的圆. d,e,f 是这三点的坐标的多项式, 因而属于 F_0. 不妨设 $b\neq 0$, 用 $y=\dfrac{-1}{b}(ax+c)$ 代入 (4) 解出得 $\alpha=A\pm\sqrt{D}$, 其中 A,D 都是 a,b,c,d,e,f 的有理分式而且 $D>0$. 于是 α 和 β 都属于 $F_0(\sqrt{D})$, z 属于 $F_0(\sqrt{D})(\sqrt{-1})=F_1(\sqrt{D})$.

iii) z 是圆 (4) 和圆 (5) 的交点

$$x^2+y^2+d'x+e'y=f'=0, \tag{5}$$

其中 (5) 也是以 S_0 中一点为圆心, 以其中两点的距离为半径的圆. (4),(5) 相减得

$$(d-d')x+(e-e')y+f-f'=0. \tag{6}$$

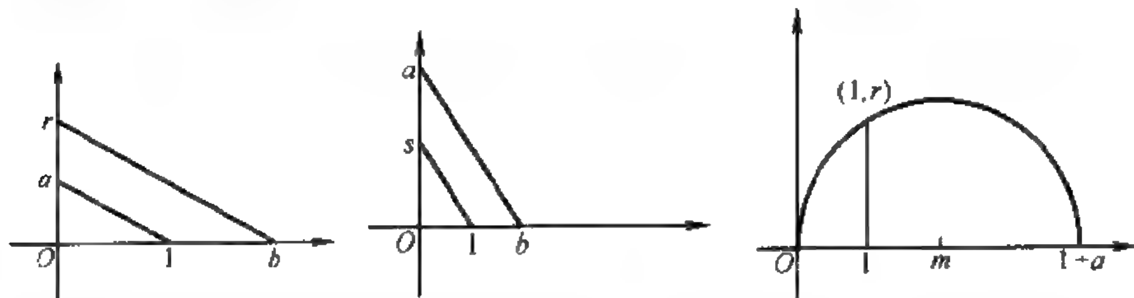
于是 z 是 (4) 和 (6) 的交, 仿 ii) 可证 z 属于 F_1 上的一个二次扩域. 其次假设 z 可以用尺规从 S_0 作出, 而且存在一串点 $z_1',\cdots,z_t'$ 且 $z_t'=z$ 使得 z_1' 可直接从 S_0 作出而且 z_{i+1}' 可直接从 $S_0\cup\{z_1',\cdots,z_i'\}$ 作出, $i=1,\cdots,t-1$. 于是对 t 作归纳法可以证明 z 属于 F_1 上的一个根式扩张 K, 而且 K/F_1 有一个二次根式扩张链 (1) 且 $t\geq r$.

其次证充分性. 先证一个

引理 设 a,b 为两个非零实数. 则 $a\pm b, a\cdot b, a/b$ 和 $\sqrt{a}$ $(a>0)$ 可以用尺规从数集 $S=\{0,1,a,b\}$ 作出.

证明 若一个实数 c 可用尺规从 S 作出, 则 $-c$ 也是这样. 因此不妨假定 $a>0,b>0$. 首先 $a+b$ 和 $a-b$ 可用尺规作出是很显然的. 其次作 $a\cdot b$. 首先将 a,b 理解为平面直角坐标系中的点 $(0,a)$ 和 $(b,0)$. 过 $(b,0)$ 作与 $(1,0)(0,a)$ 联

线平行的直线，与 y- 轴交于 $(0,r)$，则 $r=a\cdot b$. 其次作 $\frac{a}{b}$. 仍如前将 a,b 理解为 $(0,a)$ 和 $(b,0)$. 作过 $(1,0)$ 且与 $(b,0),(0,a)$ 联线平行的直线，令其与 y- 轴交于 $(0,s)$，则 $s=\frac{a}{b}$. 最后作 $\sqrt{a}$, $a>0$. 先作 $1+a$，其次作 O 和 $1+a$ 的中点 m. 然后作以 m 为圆心以 $\overline{Om}$ 为半径的圆. 最后作过 1 且与 x- 轴垂直的直线，令其与圆交于 $(1,r)$，则 $r^2=1\cdot a=a, r=\sqrt{a}$.



下面着手证明定理的充分性. 如前 $F_1=F_0(\sqrt{-1}), F_0=\mathbf{Q}(a_1,\cdots,a_n,b_1,\cdots,b_n)$, F_1 的每个数 $z=a+b\sqrt{-1}$，其中 a,b 都是 a_i 和 b_i 的有理分式，系数属于 $\mathbf{Q}$. 因为 a_i,b_i 和有理数都可从 S_0 作出，根据引理， a,b 也可从 S_0 作出，因而 z 也是这样. 其次设 $F_2=F_1(\theta),\theta^2\in F_1,[F_2:F_1]=2$. 令 $\theta=\alpha+\beta\sqrt{-1},\theta^2=a+b\sqrt{-1},a,b\in F$. 由计算

$$\alpha^2=\frac{1}{2}\left(a+\sqrt{a^2+b^2}\right),\quad \beta^2=\frac{1}{2}\left(-a+\sqrt{a^2+b^2}\right),$$

根据引理， α 和 β 可以用尺规从 S_0 作出，因而 θ 也可以从 S_0 作出. 另一方面 $F_1(\sqrt{a^2+b^2},\alpha)=F_0(\sqrt{a^2+b^2},\alpha)(\sqrt{-1})$ 而且 $F_0(\sqrt{a^2+b^2},\alpha)$ 根据引理可用尺规从 S_0 作出，因而 $F_1(\sqrt{a^2+b^2},\alpha)$ 也可用尺规从 S_0 作出. 由于 F_2 包含在 $F_1(\sqrt{a^2+b^2},\alpha)$ 内所以 F_2 可以用尺规从 S_0 作出. 然后对 r 作归纳法，就证明了充分性. □

推论 如果复数 z 可以用尺规从 $S_0=\{0,1,z,\cdots,z_n\}$ 作出，则 z 是域 $F=\mathbf{Q}(z_1,\cdots,z_n,\overline{z}_1,\cdots,\overline{z}_n)$ 上的一个代数元而且 z 的次数为 2 的方幂.

证明 设 z 可以用尺规从 $S_0=\{0,1,z_1,\cdots,z_n\}$ 作出，则 z 包含在根式扩张 K/F 中， K/F 有二次根式扩张链

$$F\subset F(\sqrt{-1})=F_1\subset F_2\subset\cdots\subset F_r=K,$$

其中后一项是前一项的二次扩张. 于是 $[K:F]=2^{r+1}$. 设 z 在 F 上的次数为 s. 则 $[F(z):F]=s$. 由 $F(z)$ 包含在 K/F 中，有 $[F(z):F]=s|[K:F]=2^{r-1}$, 所以 s 为 2 的方幂 $s=2^m$, $m\leq r$. □

以上关于尺规作图的讨论完全没有涉及到伽罗瓦理论. 如果应用伽罗瓦理论于上面的讨论，则得另一个判别准则.

定理 17 任给 $n\ (n\geq 0)$ 个复数 $z_1,\cdots,z_n$, 令 $F=\mathbf{Q}(z_1,\cdots,z_n,\bar{z}_1,\cdots,\bar{z}_n)$. 复数 z 可用尺规从 $S_0=\{0,1,z_1,\cdots,z_n\}$ 作图的充要条件是 z 包含在 F 上一个有限伽罗瓦扩张 E/F 中, 而且伽罗瓦群 $\mathrm{Gal}(E/F)$ 是一个 2^m 阶群.

证明 必要性. 设 z 可用尺规从 $S_0=\{0,1,z_1,\cdots,z_n\}$ 作出, 则 z 包含在一个根式扩张链

$$F\subset F(\sqrt{-1})=F_1\subset F_2\subset\cdots\subset F_r=K,\ [F_{i+1}:F_i]=2$$

中, 根据 §4 的引理, K/F 的正规闭包 E/F 是一个 2^m 次伽罗瓦扩张. 反之, 设复数 z 包含在一个次数为 2^m 的伽罗瓦扩张 K/F 中. 令 $G=\mathrm{Gal}(K/F)$, 则 $|G|=2^m$. 因而 G 是可解的. 于是 G 有一个合成群列

$$G=G_0\supset G_1\supset\cdots\supset G_m=\{1\},\ \ [G_i:G_{i+1}]=2.$$

在伽罗瓦对应下令 K/F 的中间域 F_i 与子群 G_i 对应. 于是得到 K/F 的一个二次根式扩张链

$$F=F_0'\subset F_1'\subset\cdots\subset F_m'=K,\ \ [F_{i+1}':F_i']=2.\tag{7}$$

当然 z 也包含在二次根式扩张链中

$$F(\sqrt{-1})\subset F_1'(\sqrt{-1})\subset\cdots\subset F_m'(\sqrt{-1})=K(\sqrt{-1}),$$

其中 $F(\sqrt{-1})$ 就是定理 16 中的 F_1, 而且 $[F_{i+1}'(\sqrt{-1}):F_i'(\sqrt{-1})]\leq 2$. 所以 z 可以用尺规从 S_0 作出. □

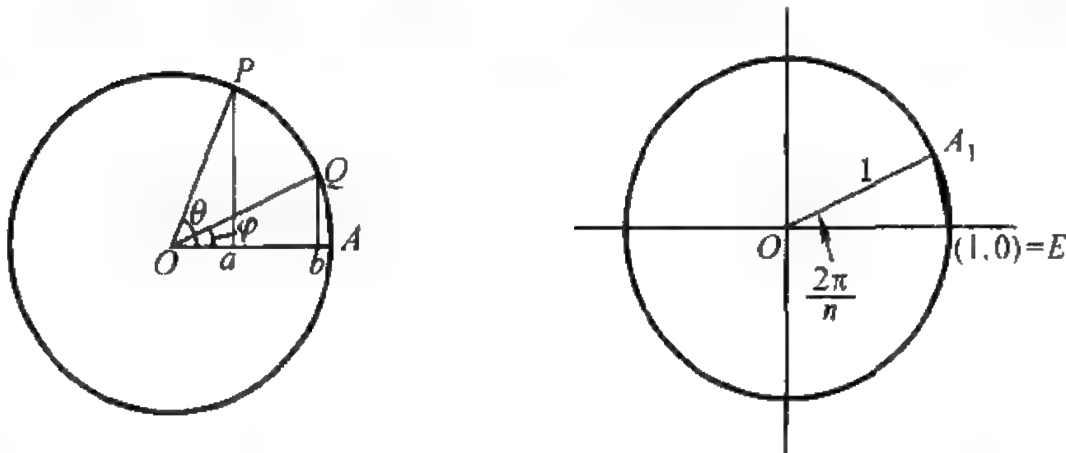
用直尺与圆规三等分任一角是平面几何作图的三大难题之一. 在 19 世纪 30 年代已经证明其不可能. 现在作为应用给出证明如下.

任意给定一个角 θ, 不妨设为锐角. 用尺规求作一个角 φ 使得 $3\varphi=\theta$. 我们证明这是不可能的. 首先需将问题变换一下使之适合应用定理 16. 将角 θ 放在一个单位圆内, 角顶点与圆心重合 (如下页左图)$\angle POA=\theta, Pa\perp OA, \angle QOA=\varphi, Qb\perp OA$. $\overline{Oa}=a=\cos\theta, \overline{Ob}=b=\cos\varphi$. θ 已知即 a 已知, φ 是待求的量也即 b 是待求的量. 现在问题就化成: 用尺规从 $\{0,1,a\}$ 作出 b. 证明这是不可能的. 由三角函数公式知

$$\cos\theta=\cos 3\varphi=4\cos^3\varphi-3\cos\varphi.$$

于是 b 是 $f(x)=4x^3-3x-\cos\theta$ 的根. 我们指出 $f(x)$ 在 $\mathbf{Q}(a)$ 上不可约. 取 θ 的一个特殊值 $\theta=\dfrac{\pi}{3}$. 此时 $\cos\theta=\dfrac{1}{2}, \mathbf{Q}(a)=\mathbf{Q}\left(\dfrac{1}{2}\right)=\mathbf{Q}, f(x)=4x^3-3x-\dfrac{1}{2}=$

$\frac{1}{2}(8x^3-6x-1)=\frac{1}{2}((2x)^3-3\cdot(2x)-1)$. 显然 $f(x)$ 在 $\mathbf{Q}$ 上不可约. 所以，一般情况的 $f(x)$ 在 $\mathbf{Q}(a)$ 上也是不可约的. 由此可知 b 是 $\mathbf{Q}(a)$ 上的一个 3 次代数元. 根据定理 16 的推论，我们得到结论： $\cos\frac{\theta}{3}$ 用尺规从 $\{0,1,\cos\theta\}$ 作出一般说来是不可能的. 这就证明了在平面上用尺规三等分任一角是不可能的.



下面讨论一个正 n $(n>2)$ 边形用尺规作图的可能性问题. 一个 n $(n>2)$ 边形叫做一个正 n 边形，如果它的各边长相等而且各顶角相等. 因而一个正 n 边形各边的垂直平分线交于一点. 这点叫做正 n 边形的中心. 以中心为圆心，以中心至顶点的距离为半径做圆，则正 n 边形的各顶点位于圆周上而且将圆周分为 n 等份，每份所对的圆心角 $=\frac{2\pi}{n}$. 正 n 边形是否可用尺规作图只与边数有关而与顶点至中心的距离无关. 因此不妨假定正 n 边形的顶点位于一个单位圆周上，中心位于坐标原点，有一个顶点与单位点 $E=(1,0)$ 重合， A_1 是与 $(1,0)$ 相邻且位于上半平面的顶点 (如上右图). 因而 $\angle A_1OE=\frac{2\pi}{n}$, A_1 的坐标为 $\left(\cos\frac{2\pi}{n},\sin\frac{2\pi}{n}\right)$, A_1 的复数表示为 $\zeta=\cos\frac{2\pi}{n}+\sqrt{-1}\sin\frac{2\pi}{n}$. 正 n 边形的 n 个顶点 $A_1,A_2,\cdots,A_n=E$(反时针方向) 的复数表示依次为 $\zeta,\zeta^2,\cdots,\zeta^n=1$. ζ 为一个本原的 n 次单位根. 正 n 边形能用尺规作出当而且仅当顶点 A_1 可用尺规从数集 $\{0,1\}$ 作出. 现在看一下 ζ 的次数. 已知 ζ 的极小多项式是 n 次分圆多项式 $\Phi_n(x)$, 它的次数 $=\varphi(n)$. 令 n 的分解式为 $2^ep_1^{e_1}\cdots p_r^{e_r}$, $p_1,\cdots,p_r$ 为不同的奇素数 $e\geq 0,e_i\geq 1,i=1,\cdots,r$. 于是

$$\varphi(n)=\begin{cases} p_1^{e_1-1}\cdots p_r^{e_r-1}(p_1-1)\cdots(p_r-1), & e=0,\\ 2^{e-1}p_1^{e_1-1}\cdots p_r^{e_r-1}(p_1-1)\cdots(p_r-1), & e>0.\end{cases}$$

定理 18 正 n $(n>2)$ 边形可用尺规作图的充要条件是 n 有分解式 $n=2^ep_1p_2\cdots p_r$, 其中 $e\geq 0,p_1,\cdots,p_r$ 为不同的费马素数.

证明 必要性. 假设正 n 边形可用尺规作图, 则本原 n 次单位根 ζ 可用尺规从 $\{0,1\}$ 作出. 根据定理 16 的推论, ζ 的次数 $\varphi(n)$ 为 2 的方幂, 从而推出 $e_1 = \cdots = e_r = 1$ 而且 $p_i - 1 = 2^{r_i}$, 即 $p_i = 1 + 2^{r_i}$ 全为费马素数. 反之, 设 $n = 2^e p_1 \cdots p_r$, 其中 $e \geq 0, p_1, \cdots, p_r$ 全为费马素数. 于是 n 分圆域 $E = \mathbf{Q}(\zeta)$ 的次数为 $\varphi(n) = 2^{e-1}(p_1 - 1)\cdots(p_r - 1)$ 或 $\varphi(n) = (p_1 - 1)\cdots(p_r - 1)$ (按 $e > 0$ 或 $e = 0$ 而定), 总之, $\varphi(n)$ 是 2 的方幂, 设 $\varphi(n) = 2^m$. 根据本章定理 9, $E/\mathbf{Q}$ 是一个伽罗瓦扩张, 而且次数 $[E:\mathbf{Q}] = 2^m$. 根据定理 17, ζ 可以用尺规从 $\{0,1\}$ 作出. 因而正 n 边形可用尺规作图. □

已知的费马素数有 3, 5, 17, 257 和 65537.

例 1 计算本原的 5 次单位根. 它们是 $x^4 + x^3 + x^2 + x + 1$ 的根. 设 ζ 为其一根, 则其它三根为 $\zeta^2, \zeta^3, \zeta^4$. 令 $\eta_1 = \zeta + \zeta^4, \eta_2 = \zeta^2 + \zeta^3$. 由计算有 $\eta_1 + \eta_2 = -1, \eta_1 \cdot \eta_2 = \eta_1 + \eta_2 = -1$. $\eta_1\eta_2$ 是方程

$$x^2 + x - 1 = 0$$

的根. 解出得

$$\eta_1 = \frac{1}{2}\left(-1 + \sqrt{5}\right), \quad \eta_2 = \frac{1}{2}\left(-1 - \sqrt{5}\right).$$

ζ 和 ζ^4 是方程

$$x^2 - \frac{1}{2}\left(-1 + \sqrt{5}\right)x + 1 = 0$$

的根, 解出得

$$\zeta = \frac{1}{4}\left(-1 + \sqrt{5} + \sqrt{2(5+\sqrt{5})}\sqrt{-1}\right),$$
$$\zeta^4 = \frac{1}{4}\left(-1 + \sqrt{5} - \sqrt{2(5+\sqrt{5})}\sqrt{-1}\right).$$

由于 ζ 的实部和虚部都是正的, ζ 落在第一象限. 因而 $\zeta = \cos\dfrac{2\pi}{5} + \sqrt{-1}\sin\dfrac{2\pi}{5}$. 其它三根为 $\zeta^2, \zeta^3, \zeta^4$. ζ^4 已有明显表达式, ζ^2 和 ζ^3 的明显表达式为

$$\zeta^2 = \frac{1}{4}\left(-(1+\sqrt{5}) + \sqrt{2(5-\sqrt{5})}\sqrt{-1}\right),$$
$$\zeta^3 = \frac{1}{4}\left(-(1+\sqrt{5}) - \sqrt{2(5-\sqrt{5})}\sqrt{-1}\right).$$

根据 ζ 的表达式就可用尺规作出正五边形的顶点 ζ.

例 2 计算本原 17 次单位根. 设 ζ 为一个本原 17 次单位根. 它的极小多项式 $f(x) = x^{16} + x^{15} + \cdots + x + 1$, 其它 15 个根为 $\zeta^i, i = 2, 3, \cdots, 16$. 令 $E = \mathbf{Q}(\zeta)$. 则 $E/\mathbf{Q}$ 为一个 16 次伽罗瓦扩张, 它的伽罗瓦群 G 和乘法群 $(\mathbf{Z}/17\mathbf{Z})^*$ 同构.

3 是 mod 17 的一个原根. 于是 G 含有一个 σ 使得 $\sigma(\zeta)=\zeta^3$. $\sigma^i(\zeta)=\zeta^{3^i}, i=0,1,\cdots,15$. σ 是 G 的一个生成元, $G=\langle\sigma\rangle$. G 有合成群列

$$G=\langle\sigma\rangle\supset\langle\sigma^2\rangle\supset\langle\sigma^4\rangle\supset\langle\sigma^8\rangle\supset\{1\},$$

与之对应的 $E/\mathbf{Q}$ 的中间域记为

$$\mathbf{Q}=F_0\subset F_1\subset F_2\subset F_3\subset F_4=E.$$

F_{i+1}/F_i 是二次扩张, $i=0,1,2,3$. 下面来定出这些中间域, 同时也就解出 $f(x)$ 的根. $f(x)$ 的根在群 G 的作用下成一个传递集. 将群缩小到 $\langle\sigma^2\rangle$, 这 16 个根在 $\langle\sigma^2\rangle$ 的作用下分解成两个传递集, 其中一个是 $\{\zeta,\sigma^2(\zeta),\sigma^4(\zeta),\cdots,\sigma^{14}(\zeta)\}$. 对它们求和

$$x_1=\zeta+\sigma^2(\zeta)+\cdots+\sigma^{15}(\zeta).$$

另一个传递集的和则是

$$\sigma(x_1)=\sigma(\zeta)+\sigma^3(\zeta)+\cdots+\sigma^{15}(\zeta).$$

x_1 与 $\sigma(x_1)$ 在 G 下成一传递集. 由计算

$$x_1+\sigma(x_1)=\sum_{i=0}^{15}\sigma^i(\zeta)=-1,$$

$$x_1\cdot\sigma(x_1)=4\sum_{i=0}^{15}\sigma^i(\zeta)=-4.$$

第一式显然, 第二式需要解释一下. 由于 $3^8\equiv-1\pmod{17}$, $\sigma^i(\zeta)$ 与 $\sigma^{i+8}(\zeta)$ 互为逆元素: $\sigma^i(\zeta)\cdot\sigma^{i+8}(\zeta)=\sigma^i(\zeta)\cdot\sigma^i(\zeta^{3^8})=\sigma^i(\zeta)\cdot\sigma^i(\zeta^{-1})=\sigma^i(\zeta\cdot\zeta^{-1})=1$. 因而 $\sigma^i(\zeta)$ 与 $\sigma^{i+8}(\zeta)$ 属于同一个传递集. 因而 x_1 中每一项与 $\sigma(x_1)$ 中每一项相乘不等于 1. $x_1\cdot\sigma(x_1)$ 只能是 $\zeta,\zeta^2,\cdots,\zeta^{16}$ 的线性组合, 设 $x_1\cdot\sigma(x_1)=\sum\limits_{i=1}^{16}a_i\zeta^i$. 注意 $x_1\sigma(x_1)$ 是 G 的不动元, 因而属于 $\mathbf{Q}$; 另一方面, $\zeta,\zeta^2,\cdots,\zeta^{16}$ 在 $\mathbf{Q}$ 上仅有一个基本关系 $\zeta+\zeta^2+\cdots+\zeta^{16}=-1$, 从而推出 $a_1=a_2=\cdots=a_{16}$, 比较等式两边的项数, 知 $a_i=4$. 这表明 x_1 和 $\sigma(x_1)$ 是方程

$$x^2+x-4=0$$

的根. 方程有两个解: $\frac{1}{2}(-1\pm\sqrt{17})$. x_1 取哪一个解? 我们的目的是求出具体的 16 个根 $\cos\frac{2k\pi}{17}+i\sin\frac{2k\pi}{17}, k=1,2,\cdots,16$ 中的一个. 至于是哪一个对我们

是无关紧要的. 当我们令 x_1 取定其中一解, 这只表明将来解出的 ζ 属于上面两个传递集中的一个. 如果 x_1 取另一解, 那么将来解出的 ζ 则属于另一个传递集. 因此不妨取

$$x_1 = \frac{1}{2}(1+\sqrt{17}), \sigma(x_1) = \frac{1}{2}(1-\sqrt{17}). \tag{8}$$

此时 $\mathbf{Q}(x_1)$ 包含在 $\langle\sigma^2\rangle$ 的不动域 F_1 中. 比较次数知 $F_1 = \mathbf{Q}(x_1)$. 仿上, x_1 的项和 $\sigma(x_1)$ 的项在 $\langle\sigma^4\rangle$ 下各分解成两个传递集. 这四个传递集的和可表成

$$\begin{aligned} y_1 &= \zeta + \sigma^4(\zeta) + \sigma^8(\zeta) + \sigma^{12}(\zeta), \\ \sigma^2(y_1) &= \sigma^2(\zeta) + \sigma^6(\zeta) + \sigma^{10}(\zeta) + \sigma^{14}(\zeta), \\ \sigma(y_1) &= \sigma(\zeta) + \sigma^5(\zeta) + \sigma^9(\zeta) + \sigma^{13}(\zeta), \\ \sigma^3(y_1) &= \sigma^3(\zeta) + \sigma^7(\zeta) + \sigma^{11}(\zeta) + \sigma^{15}(\zeta). \end{aligned}$$

$\sigma^i(y_1)$ 都是 $\langle\sigma^4\rangle$ 的不动元. 但是 y_1 和 $\sigma^2(y_1)$($\sigma(y_1)$ 和 $\sigma^3(y_1)$) 构成 $\langle\sigma^2\rangle$ 的传递集. 为了计算, 将 $\sigma^i(\zeta) = \zeta^{3^i}$ 写成 $\sigma^i(\zeta) = \zeta^{k_i}$, $1 \le k_i < 17$, 则 $\sigma^i(y_1)$ 可表成

$$\begin{aligned} y_1 &= \zeta + \zeta^{13} + \zeta^{16} + \zeta^4, \\ \sigma^2(y_1) &= \zeta^9 + \zeta^{15} + \zeta^8 + \zeta^2, \\ \sigma(y_1) &= \zeta^3 + \zeta^5 + \zeta^{14} + \zeta^{12}, \\ \sigma^3(y_1) &= \zeta^{10} + \zeta^{11} + \zeta^7 + \zeta^6. \end{aligned}$$

由计算, $y_1 + \sigma^2(y_1) = x_1, y_1 \cdot \sigma^2(y_1) = -1$, y_1 与 $\sigma^2(y_1)$ 是方程

$$x^2 - x_1 x - 1 = 0$$

的根. 和上面出现的问题一样, y_1 的值有两种取法. 理由不再说明, 请读者自己思考. 不妨取

$$y_1 = \frac{1}{2}\left(x_1 + \sqrt{x_1^2+4}\right), \quad \sigma^2(y_1) = \frac{1}{2}\left(x_1 - \sqrt{x_1^2+4}\right), \tag{9}$$

$F_1(y_1)$ 包含在 $\langle\sigma^4\rangle$ 的不动域 F_2 内, 比较次数得 $F_2 = F_1(y_1)$. 为了下面的需要, 还要计算 $\sigma(y_1)$ 与 $\sigma^3(y_1)$. 实际上, 当 y_1 的值一经取定之后, 由于 $\sigma(y_1), \sigma^3(y_1) \in F_1(y_1)$, $\sigma(y_1)$ 与 $\sigma^3(y_1)$ 的值也就定了. 由计算知 $x_1 y_1 = 3 + \sigma^2(y_1) + 2\sigma(y_1)$. 于是 $2\sigma(y_1) = x_1 y_1 - \sigma^2(y_1) - 3$. 用 (9) 代入, 化简得

$$\sigma(y_1) = \frac{1}{2}\left(\sigma(x_1) + \sqrt{\sigma(x_1)^2+4}\right). \tag{10}$$

由于 $\sigma(y_1)$ 与 $\sigma^3(y_1)$ 为方程 $x^2 - \sigma(x_1)x - 1 = 0$ 的根, 所以 $\sigma^3(y)$ 是另一根

$$\sigma^3(y_1) = \frac{1}{2}\left(\sigma(x_1) - \sqrt{\sigma(x_1)^2+4}\right).$$

再进一步，y_1 的项在 $\langle\sigma^8\rangle$ 下分解成两个传递集 $\{\zeta,\sigma^8(\zeta)\}$ 和 $\{\sigma^4(\zeta),\sigma^{12}(\zeta)\}$. 令

$$z_1=\zeta+\sigma^8(\zeta),\quad \sigma^4(z_1)=\sigma^4(\zeta)+\sigma^{12}(\zeta).$$

由计算 $z_1+\sigma^4(z_1)=y_1, z_1\cdot\sigma^4(z_1)=\sigma(y_1)$, z_1 和 $\sigma^4(z_1)$ 是方程

$$x^2-y_1x+\sigma(y_1)=0$$

的根. 和上面一样，z_1 的值有两种取法，不妨取

$$\begin{aligned} z_1&=\frac{1}{2}\left(y_1+\sqrt{y_1^2-4\sigma(y_1)}\right),\\ \sigma^4(z_1)&=\frac{1}{2}\left(y_1-\sqrt{y_1^2-4\sigma(y_1)}\right). \end{aligned}\tag{11}$$

同样，$F_2(z_1)$ 是 $\langle\sigma^8\rangle$ 的不动域，$F_2(z_1)=F_3$. 到现在为止求出的中间域 F_3 是 E 的实子域而且是 E 的最大实子域. 次数 $[F_3:\mathbf{Q}]=8, [E:F_3]=2$. 最后，$\zeta$ 和 $\sigma^8(\zeta)=\zeta^{-1}$ 是方程

$$x^2-z_1x+1=0$$

的根. ζ 的值也有两种取法，不妨取

$$\zeta=\frac{1}{2}\left(z_1+\sqrt{z_1^2-4}\right)=\frac{1}{2}\left(z_1+\sqrt{4-z_1^2}\sqrt{-1}\right).\tag{12}$$

这样就将求解 ζ 的问题化为求解一串二次方程的问题. 只要依次解出 (8)~(12), 就得到了 ζ 的根式解，其中只含 2 次根式. 因此，ζ 可用尺规从 $\{0,1\}$ 作得. 从而正十七边形的全部顶点都可作出. （读者想一想，为什么？）

§7 具有对称群的整系数多项式的存在

我们已经知道一个无重根的 n 次多项式 $f(x)$ 的伽罗瓦群是 n 文字对称群 S_n 的一个子群. 自然要问它的反问题：对 S_n 的任一子群 H, 是否存在一个 n 次整系数多项式 $f(x)$ 使得它的伽罗瓦群就是 H? 这是一个至今还未解决的问题. 在本节我们将证明，当 $H=S_n$ 时，答案是肯定的.

设 $f(x)$ 是域 F 上一个无重根的多项式，E/F 为它的分裂域. 将 E/F 的伽罗瓦群视为 $f(x)$ 的 n 个根的置换群. 下面给出确定这个群的一般方法. 设 $u_1,\cdots,u_n$ 为 F 上 n 个独立未定元，$K=F(u_1,\cdots,u_n)$ 为有理分式域. 根据定理 3, 可作 E 和 K 在 F 上的复合域 $L=E\cdot K$, L 是 K 上的伽罗瓦扩张，且是 $f(x)$ 在 K 上的分裂域. 而且 $\mathrm{Gal}(L/K)\cong\mathrm{Gal}(E/E\cap K)$. 由于 E 的元素在 F

上都是代数的而 K 中 F 以外的每个元素在 F 上都是超越的, 因而 $E\cap K=F$. 所以

$$\mathrm{Gal}(E\cdot K/K)\cong \mathrm{Gal}(E/F).$$

其次定出 $\mathrm{Gal}(L/K)$. L 包含一个元素

$$\theta=\alpha_1u_1+\alpha_2u_2+\cdots+\alpha_nu_n,$$

其中 $\alpha_1,\cdots,\alpha_n$ 为 $f(x)$ 的根. S_n 的每个置换 π 对 θ 的作用规定为

$$\pi\theta=\alpha_{\pi(1)}u_1+\alpha_{\pi(2)}u_2+\cdots+\alpha_{\pi(n)}u_n.$$

对任意 $\pi,\pi'\in S_n$, 显然有 $\pi\theta=\pi'\theta$ 当且仅当 $\pi=\pi'$. 因此 θ 在 S_n 的作用下是 $n!$ 值函数. 作

$$G(x)=\prod_{\pi\in S_n}(x-\pi\theta).$$

$G(x)$ 的系数是 $u_1,\cdots,u_n$ 的齐次多项式, 这些齐次多项式的系数都是 $\alpha_1,\cdots,\alpha_n$ 的对称函数, 因而都属于 F. 所以 $G(x)$ 的系数全属于 K. 令 $G(x)$ 在 K 上分解成不可约因式的积

$$G(x)=g_1(x)g_2(x)\cdots g_r(x).$$

并约定 θ 是 $g_1(x)$ 的根.

定理 19 *设 E/F 为无重根的 n 次多项式 $f(x)$ 的分裂域, $K=F(u_1,\cdots,u_n)$ 为 n 个独立未定元的分式域, 则*

1) $\mathrm{Gal}(E/F)=\mathrm{Gal}(E\cdot K/K)$, *记作 G.*

2) *令 $\theta=\alpha_1u_1+\cdots+\alpha_nu_n$, $\alpha_1,\cdots,\alpha_n$ 为 $f(x)$ 的根, 已知 $g_1(x)$ 为 θ 在 K 上的极小多项式. 则对于每个 $\pi\in S_n$, π 属于 G 当且仅当 $\pi\theta$ 也是 $g_1(x)$ 的根.*

3) $E\cdot K=K(\theta)$.

证明 1) 已经证明在上面. 证明 2). 若 $\pi\in G$, 则 π 是 $E\cdot K$ 的一个 K- 自同构. 于是 θ 和 $\pi\theta$ 有相同的极小多项式 (§1 引理 4) 因而 $g_1(\pi\theta)=0$. 反之, 若 $g_1(\pi\theta)=0$, 则同样根据 §1, 引理 4, $E\cdot K$ 有一个 K- 自同构 σ 使得 $\sigma(\theta)=\pi\theta$. 由于 $\sigma(u_i)=u_i$, $\sigma(\theta)=\sigma(\alpha_1)u_1+\cdots+\sigma(\alpha_n)u_n=\pi\theta=\alpha_{\pi(1)}u_1+\cdots+\alpha_{\pi(n)}u_n$, 得 $\sigma(\alpha_i)=\alpha_{\pi(i)}$, 所以 $\pi=\pi_\sigma\in G$.

3) 若 $\pi\in G$ 保持 θ 不动, 即 $\pi\theta=\theta$, 从而 $\alpha_{\pi(1)}u_1+\cdots+\alpha_{\pi(n)}u_n=\alpha_1u_1+\cdots+\alpha_nu_n$, 但是 $u_1,\cdots,u_n$ 在 K 上线性无关, 推得 $\pi(i)=i$, $i=1,\cdots,n$, $\pi=e$. 所以与 $K(\theta)$ 对应的 G 的子群为单位元群. 根据伽罗瓦基本定理, $K(\theta)=E\cdot K$. □

说明 由 2) 的证明可知，2) 的结论与 θ 的选取是无关的，就是说任取 $G(x)$ 的一根充当 θ, 2) 的结论对 θ 来说仍然成立.

以下考虑有理数域 $\mathbf{Q}$ 上一个无重根的 n 次多项式 $f(x)$ 的群. 此时不妨假定 $f(x)$ 的系数全为整数而且首项系数为 1. 令 $E/\mathbf{Q}$ 为 $f(x)$ 的分裂域. $E = \mathbf{Q}(\alpha_1,\cdots,\alpha_n)$, $\alpha_1,\cdots,\alpha_n$ 为 $f(x)$ 的全部根. $f(x)$ 的判别式 $D(f) = \prod\limits_{i<j}(\alpha_i-\alpha_j)^2$ 为整数. 任取一个素数 p, 只要求它与 $D(f)$ 互素. 在自然同态 $\mathbf{Z}\to\mathbf{F}_p$ 下 $f(x)$ 的象记作 $\overline{f}(x)$. 用同余式的话来说，$\overline{f}(x)$ 等于 $D(f)$ (mod p). 由于 p 与 $D(f)$ 互素而且 $\overline{f}(x)$ 的判别式 $D(\overline{f})$ 等于 $f(x)$ (mod p). 后者不同余 0, 因而 $D(\overline{f})\neq 0$, $\overline{f}(x)$ 是一个无重根的 n 次多项式. 我们来阐明 $f(x)$ 在 $\mathbf{Q}$ 上的群和 $\overline{f}(x)$ 在 $\mathbf{F}_p$ 上的群之间的关系. 设 $\overline{E}/\mathbf{F}_p$ 为 $\overline{f}(x)$ 的分裂域，$\overline{E} = \mathbf{F}_p(\overline{\alpha}_1,\cdots,\overline{\alpha}_n)$, $\overline{\alpha}_1,\cdots,\overline{\alpha}_n$ 为 $\overline{f}(x)$ 的全部根. 这里的 $\overline{\alpha}_i$ 并没有 "$\overline{\alpha}_i$ 等于 α_i (mod p)" 的意思，更何况 α (mod p) 还没有定义，而且也不能这样定义. 因此我们不去管 α_i 与 $\overline{\alpha}_i$ 有无内在的联系，只注意 $f(x)$ 的根和 $\overline{f}(x)$ 的根有一个一一对应 $\alpha_i\to\overline{\alpha}_i$ 就够了. 重要的是它们的对称多项式有确定的同余关系.

引理 1 *设 $\varphi(\alpha_1,\cdots,\alpha_n)$ 为 $\alpha_1,\cdots,\alpha_n$ 的对称多项式而且系数为整数. 则 $\varphi(\overline{\alpha}_1,\cdots,\overline{\alpha}_n)$ 等于 $\varphi(\alpha_1,\cdots,\alpha_n)$ (mod p).*

证明 设 $f(x) = x^n + a_1x^{n-1}+\cdots+a_n$, 则 $\overline{f}(x) = x^n+\overline{a}_1x^{n-1}+\cdots+\overline{a}_n$, 且 $(-1)^ia_i = \sum\alpha_1\alpha_2\cdots\alpha_i$, $(-1)^i\overline{a}_i = \sum\overline{\alpha}_1\overline{\alpha}_2\cdots\overline{\alpha}_i$ $(i=1,\cdots,n)$ 为初等对称多项式. 根据对称多项式的基本定理，$\varphi(\alpha_1,\cdots,\alpha_n)$ 可表成 $-a_1,a_2,\cdots,(-1)^na_n$ 的多项式 $g(-a_1,a_2,\cdots,(-1)^na_n)$, 而且系数为整数: $\varphi(\alpha_1,\cdots,\alpha_n) = g(-a_1,\cdots,(-1)^na_n)$. 这是 $\alpha_1,\cdots,\alpha_n$ 的一个恒等式. 用 $\overline{\alpha}_i$ 代入 α_i, $i=1,\cdots,n$ 得

$$\varphi(\overline{\alpha}_1,\overline{\alpha}_2,\cdots,\overline{\alpha}_n) = g(-\overline{a}_1,\overline{a}_2,\cdots,(-1)^n\overline{a}_n).$$

由于 a_i 为整数，$\overline{a}_i$ 等于 a_i (mod p), 而且 $g(-a_1,\cdots,(-1)^na_n)$ 的系数为整数. 于是 $g(-\overline{a}_1,\cdots,(-1)^n\overline{a}_n)$ 等于 $g(-a_1,\cdots,(-1)^na_n)$ (mod p). 就是说 $\varphi(\overline{\alpha}_1,\cdots,\overline{\alpha}_n)$ 等于 $\varphi(\alpha_1,\cdots,\alpha_n)$ (mod p). □

现在应用定理 19 于 $E/\mathbf{Q}$ 和 $\overline{E}/\mathbf{F}_p$. 在 $\mathbf{Q}$ 上引进 n 个独立未定元 $u_1,\cdots,u_n$, 令 $K=\mathbf{Q}(u_1,\cdots,u_n)$, $L=E(u_1,\cdots,u_n)$. 于是 $\mathrm{Gal}(L/K)\cong\mathrm{Gal}(E/\mathbf{Q})$. 作

$$\theta = \alpha_1u_1+\cdots+\alpha_nu_n,$$
$$G(x) = \prod_{\pi\in S_n}(x-\pi\theta).$$

在 K 上 $G(x)$ 分解成不可约因式

$$G(x) = g_1(x)\cdots g_r(x),$$

其中 θ 为 $g_1(x)$ 的一根. 同样在 $\mathbf{F}_p$ 上引进同样的独立未定元 $u_1,\cdots,u_n$. 令 $\overline{K}=\mathbf{F}_p(u_1,\cdots,u_n)$, $\overline{L}=\overline{E}(u_1,\cdots,u_n)$. 于是 $\mathrm{Gal}(\overline{E}/\mathbf{F}_p)\cong\mathrm{Gal}(\overline{L}/\overline{K})$. 令

$$\overline{\theta}=\overline{\alpha}_1u_1+\cdots+\overline{\alpha}_nu_n,$$
$$H(x)=\prod_{\pi\in S_n}(x-\pi\overline{\theta}).$$

在 $\overline{K}$ 上 $H(x)$ 分解成不可约因式

$$H(x)=h_1(x)\cdots h_s(x),$$

其中 $\overline{\theta}$ 为 $h_1(x)$ 的根. 根据引理 1 可知, $H(x)$ 等于 $G(x)\ (\mathrm{mod}\ p)$. 让 $g_i(x)\ (\mathrm{mod}\ p)$ 记作 $\overline{g}_i(x)$. 于是 $H(x)$ 在 $\overline{K}$ 上有分解

$$H(x)=\overline{g}_1(x)\cdots\overline{g}_r(x),$$

其中 $\overline{\theta}$ 是 $\overline{g}_1(x)$ 的根. 由于 $h_1(x)$ 在 $\overline{K}$ 上不可约且与 $\overline{g}_1(x)$ 有公根 $\overline{\theta}$, 因而 $h_1(x)|\overline{g}_1(x)$.

定理 20 *设 $f(x)$ 为有理数域 $\mathbf{Q}$ 上一个无重根的 n 次整系数多项式, 而且首项系数为 1. 令 p 为任一与 $f(x)$ 的判别式 $D(f)$ 互素的素数, 并令 $\overline{f}(x)$ 表示 $f(x)\ (\mathrm{mod}\ p)$. 于是 $\overline{f}(x)$ 在特征 p 素域 $\mathbf{F}_p$ 上的群 N 是 $f(x)$ 在 $\mathbf{Q}$ 上的群 G 的一个子群.*

证明 对于任一 $\pi\in N$, 根据定理 19, $\pi\overline{\theta}$ 和 $\overline{\theta}$ 适合相同的多项式 $h_1(x)$. 即 $h_1(\pi\overline{\theta})=0$. 由于 $h_1(x)|\overline{g}_1(x)$, 有 $\overline{g}_1(\pi\overline{\theta})=0$. 由引理 1 可知 $g_1(\pi\theta)=0$. 再根据定理 19, $\pi\in G$. □

根据 §3 可知 $f(x)\ (\mathrm{mod}\ p)$ 在 $\mathbf{F}_p$ 上的群是一个循环群, 而且是由 S_n 中的一个轮换生成的. 只要适当选取某些素数 $p_1,\cdots,p_r$ 使得 $f(x)\ (\mathrm{mod}\ p_i)$ 在 $\mathbf{F}_{p_i}$ 上的群为我们提供足够的信息就可以定出 $f(x)$ 在 $\mathbf{Q}$ 上的群. 这由下列引理可见一斑.

引理 2 *设 G 是 $n\ (n>1)$ 个文字的传递的置换群. 如果 G 包含一个对换和一个 $n-1$ 轮换, 则 G 就是 n 文字的对称群.*

证明 将文字重新标号, 可假设 G 包含的 $n-1$ 轮换是 $\tau=(1,2,\cdots,n-1)$, 包含的对换是 (ij). 由于 G 是传递的, G 含有一个置换 σ 使得 $\sigma(j)=n$. 于是 G 含有 $\sigma(ij)\sigma^{-1}=(kn)$, k 属于 $\{1,2,\cdots,n-1\}$. 从而 G 包含 $n-1$ 个对换 $\tau^\nu(kn)\tau^{-\nu}=(\tau^\nu(k)n),\nu=1,2,\cdots,n-1$. 当 ν 取遍 $1,2,\cdots,n-1$ 时, $\tau^\nu(k)$ 就同时取遍 $1,\cdots,n-1$. 因而 G 包含 $(1n),(2n),\cdots,(n-1\ n)$. 这 $n-1$ 个对换生成对称群 S_n. 所以 $G=S_n$. □

定理 21 对每个正整数 n, 恒存在 n 次不可约的整系数多项式 $f(x)$ 使得 $f(x)$ 在有理数域上的群为 n 个文字的对称群.

证明 根据 §3 可知, 对每个素数 p 来说在 p 个元素的有限域 $\mathbf{F}_p$ 上存在 n 次不可约多项式. 换句话说, 即存在 mod p 的 n 次不可约整系数多项式. 下面对 $p=2,3,5$ 来选取整系数多项式, 但总是约定首项系数为 1. 只考虑 $n>1$ 的情况. 取定一个 mod 2 的 n 次不可约多项式 $f_1(x)$. 再取定一个 mod 3 的 $n-1$ 次不可约多项式 $f_2(x)$ 而且取一个 $a=1$ 或 2 使得 $f_2(a)\neq 0 \pmod 3$. 当 n 为奇数时, 取一个 mod 5 的 2 次不可约多项式 $f_3(x)$ 和一个 mod 5 的 $n-2$ 次不可约多项式 $f_4(x)$; 当 n 为偶数时, 除取定 $f_3(x)$ 之外, 还取定一个 mod 5 的 $n-3$ 次不可约多项式 $f_5(x)$ 和一个 $b=1$ 或 2 使得 $f_5(b)\neq 0 \pmod 5$. 于是构造 $f(x)$:

当 n 为奇数时, 令

$$f(x)=15f_1(x)+10(x-a)f_2(x)+6f_3(x)f_4(x).$$

当 n 为偶数时, 取

$$f(x)=15f_1(x)+10(x-a)f_2(x)+6(x-b)f_3(x)f_5(x).$$

这样作出来的 $f(x)$ 符合我们的要求. 首先 $f(x)\equiv f_1(x) \pmod 2$, 因而 $f(x)$ 是 n 次不可约的 (在有理数域 $\mathbf{Q}$ 上不可约). 设 $f(x)$ 在 $\mathbf{Q}$ 上的群为 G, 则 G 是传递的. 其次, 由于 $f(x)\equiv(x-a)f_2(x) \pmod 3$, 因而 $f(x) \pmod 3$ 只有单根而且在 $\mathbf{F}_3$ 上的分裂域 K 等于 $f_2(x) \pmod 3$ 在 $\mathbf{F}_3$ 上的分裂域 L, 而 L 是 $\mathbf{F}_3$ 上的 $n-1$ 次扩张, 根据 §3,$\mathrm{Gal}(L/\mathbf{F}_3)$ 是一个 $n-1$ 阶循环群, 所以 $f(x) \pmod 3$ 在 $\mathbf{F}_3$ 上的群 H 是一个 $n-1$ 阶循环群, 它由 S_n 中一个 $n-1$ 轮换生成. 由定理 20, $H\subset G$. 因而 G 含有一个 $n-1$ 轮换. 最后, 当 n 为偶数时, 由于 $f(x)\equiv(x-b)f_3(x)f_5(x) \pmod 5$, $f(x) \pmod 5$ 只有单根而且 $f(x) \pmod 5$ 在 $\mathbf{F}_5$ 上的分裂域 K' 等于 $f_3(x)\cdot f_5(x) \pmod 5$ 在 $\mathbf{F}_5$ 上的分裂域 L', L' 既包含 $f_3(x) \pmod 5$ 在 $\mathbf{F}_5$ 上的分裂域 $L_1/\mathbf{F}_5$, 又包含 $f_5(x)$ 在 $\mathbf{F}_5$ 上的分裂域 $L_2/\mathbf{F}_5$. 看它们的次数. $[L_1:\mathbf{F}_5]=2.[L_2:\mathbf{F}_5]=n-3$, $n-3$ 为奇数, $(n-3,2)=1$. 由 $[L_i:\mathbf{F}_5][L':\mathbf{F}_5]$ 可知 $2(n-3)|[L':\mathbf{F}_5]$. 实际上 $[L':\mathbf{F}_5]=2(n-3)$. 因而 $\mathrm{Gal}(L'/\mathbf{F}_5)$ 是一个 $2(n-3)$ 阶循环群. 所以当 n 为偶数时, $f(x) \pmod 5$ 在 F_5 上的群 H' 是一个 $2(n-3)$ 阶循环群. 由于 $[L':L_2]=2$, H' 包含一个对换. 同样根据定理 20, G 含有一个对换. 当 n 为奇数时 $f(x)\equiv f_3(x)f_4(x) \pmod 5$. 于是 $f(x) \pmod 5$ 只有单根而且在 $\mathbf{F}_5$ 上的分裂域 K'' 等于 $f_3(x)f_4(x) \pmod 5$ 在 $\mathbf{F}_5$ 上的分裂域 L''. 仿上, 由于 $\deg f_4(x)=n-2$ 为奇数, $(2,n-2)=1$. 同样得 $[L'':\mathbf{F}_5]=2(n-2)$. 因而 $f(x) \pmod 5$ 在 $\mathbf{F}_5$ 上的群 H'' 为 $2(n-2)$ 阶循环群. 由于 L'' 是 $f_4(x)$ 的分裂域上的二次扩张, G 包含一个对换. 所以当 n 为

奇数时，G 也包含一个对换. 总之 G 包含一个对换. 这样 G 既包含一个 $n-1$ 轮换又包含一个对换，而且 G 又是传递的. 由引理 2 可知，$G=S_n$. □

说明 如果在上面证明中用一个大于 3 和 $n-2$ 的素数 p 替代素数 5, 则证明要简单得多. 此时只需取一个 mod p 不可约的 2 次整系数多项式 $f_p(x)$. 简单取

$$f(x)=3pf_1(x)+2p(x-a)f_2(x)+2\cdot 3(x-1)\cdots(x-n+2)f_3(x)$$

就符合要求. 而且利用大素数容易证明有无限多个 n 次不可约整系数多项式满足定理 21 的要求.

例 1 求一个具有对称群的四次不可约整系数多项式.

解 取 $f_1(x)=x^4+x+1$. 在 $\mathbf{F}_2$ 内只有一个 2 次不可约多项式 x^2+x+1. 而 $f_1(x)$ 既没有一次因式又没有 2 次因式 x^2+x+1, 因而 $f_1(x)$ 不可约. 取 $f_2(x)=x^3-x+1$. 在 $\mathbf{F}_3[x]$ 内 $f_2(x)$ 没有一次因式，因而不可约. 取 $f_3(x)=x^2+x+1$. 在 $\mathbf{F}_5[x]$ 内 $f_3(x)$ 不可约. 令

$$\begin{aligned}f(x)=&-15(x^4+x+1)+10(x-1)(x^3-x+1)+6x(x-1)(x^2+x+1)\\=&x^4-10x^3-10x^2-x-25.\end{aligned}$$

于是 $f(x)$ 在 $\mathbf{Q}$ 上的群为 S_4.

例 2 决定 $f(x)=x^6+18x^4+6x^3+2x^2+7x-15$ 在 $\mathbf{Q}$ 上的群.

解 $f(x)\equiv x^6+x+1 \pmod 2$. 在 $\mathbf{F}_2[x]$ 内 $f_1(x)=x^6+x+1$ 没有一次因式，而且在 $\mathbf{F}_2[x]$ 内只有一个 2 次不可约多项式 x^2+x+1 和两个 3 次不可约多项式 x^3+x^2+1 和 x^3+x+1. 它们都不是 $f_1(x)$ 的因式，所以 $f_1(x)$ 不可约. 从而 $f(x)$ 在 $\mathbf{Q}$ 上也不可约. 设 G 为 $f(x)$ 在 $\mathbf{Q}$ 上的群. 其次 $f(x)\equiv x^6+2x^2+x=x(x^5+2x+1) \pmod 3$, 在 $\mathbf{F}_3[x]$ 内 $f_2(x)=x^5+2x+1$ 没有一次因式而且在 $\mathbf{F}_3[x]$ 内只有三个 2 次不可约多项式 x^2+1, x^2+x-1 和 x^2-x-1, 它们都不是 $f_2(x)$ 的因式，因而 $f_2(x)$ 不可约. 由此可知 G 含有 5 轮换. 最后，$f(x)\equiv x^6+3x^4+x^3+2x^2+2x\equiv x(x^2+2)(x^3+x+1) \pmod 5$, 其中 x^2+2 和 x^3+x+1 都是 $\mathbf{F}_5[x]$ 中不可约多项式，因而 G 含有一个对换. 根据引理 2, $G=S_6$.

§8 诺特方程与循环扩张

本节研究有限伽罗瓦扩张的伽罗瓦群的第一个上同调群. 并将它应用到循环扩张.

设 K/F 为一个 n 次伽罗瓦扩张， $G=\mathrm{Gal}(K/F)=\{\sigma_1=1,\sigma_2,\cdots,\sigma_n\}$. 根据第七章 §8 引理 1 可知，从 K 到 F 的迹和范数可写成

$$T_F^K(\alpha)=\sigma_1(\alpha)+\sigma_2(\alpha)+\cdots+\sigma_n(\alpha),$$
$$N_F^K(\alpha)=\sigma_1(\alpha)\cdot\sigma_2(\alpha)\cdots\sigma_n(\alpha).$$

定义 10 如果从 G 到乘法群 $K^*=K-\{0\}$ 的一个映射 $\eta(\sigma)$ 满足

$$\eta(\sigma\tau)=\eta(\sigma)\eta(\tau)^{\sigma}, \tag{1}$$

其中 $\eta(\tau)^{\sigma}$ 表示 $\eta(\tau)$ 在 σ 作用下的象，则称 $\eta(\sigma)$ 满足 **诺特方程**(1). 满足诺特方程的映射 η 称为 G 到 K^* 的一个 **叉同态**.

引理 1 *设 K/F 为一个有限伽罗瓦扩张， $G=\mathrm{Gal}(K/F)$. 设 $\eta:G\to K^*$ 是一个叉同态. 若 η 是一个同态，则 η 是 G 到 F^* 的一个同态；反之，任一个同态 $\eta:G\to F^*$ 是一个叉同态.*

证明 若 η 是一个叉同态同时是一个同态, 则 $\eta(\sigma\tau)=\eta(\sigma)\eta(\tau)^{\sigma}=\eta(\sigma)\eta(\tau)$, 从而 $\eta(\tau)^{\sigma}=\eta(\tau)$ 对所有 $\sigma,\tau\in G$. 从而 $\eta(\tau)\in F^*$. 反之，设 η 是一个同态 $G\to F^*$. 于是 $\eta(\sigma\tau)=\eta(\sigma)\eta(\tau)=\eta(\sigma)\eta(\tau)^{\sigma}$. 因而 η 是一个叉同态. □

引理 2 *一个有限伽罗瓦扩张 K/F 的叉同态全体，记作 Z, 对函数的乘法，成一群.*

证明 设 ξ,η 为两个叉同态. 乘法 $\xi\cdot\eta(\sigma)=\xi(\sigma)\cdot\eta(\sigma)$. 于是

$$\begin{aligned}\xi\eta(\sigma\tau)&=\xi(\sigma\tau)\eta(\sigma\tau)=\xi(\sigma)\xi(\tau)^{\sigma}\cdot\eta(\sigma)\eta(\tau)^{\sigma}\\&=\xi(\sigma)\eta(\sigma)\cdot(\xi(\tau)\eta(\tau))^{\sigma}=\xi\eta(\sigma)\cdot\xi\eta(\tau)^{\sigma},\end{aligned}$$

所以 $\xi\eta$ 还是一个叉同态. 定义 $\xi^{-1}(\sigma)=\xi(\sigma)^{-1}$. 于是

$$\begin{aligned}\xi^{-1}(\sigma\tau)&=\xi(\sigma\tau)^{-1}=(\xi(\sigma)\xi(\tau)^{\sigma})^{-1}=\xi(\sigma)^{-1}\cdot\xi(\tau)^{-\sigma}\\&=\xi^{-1}(\sigma)\cdot\xi^{-1}(\tau)^{\sigma},\end{aligned}$$

($\xi(\tau)^{-\sigma}$ 规定为 $(\xi(\tau)^{-1})^{\sigma}$)
所以 ξ 的逆 ξ^{-1} 也是一个叉同态. □

K^* 的每个元素 α 定义一个映射 $\eta_\alpha:G\to K^*$, $\eta_\alpha(\sigma)=\dfrac{\alpha^{\sigma}}{\alpha}$, $\sigma\in G$. 令 $B=\{\eta_\alpha\,|\,\alpha\in K^*\}$. 以后 $\dfrac{\alpha^{\sigma}}{\alpha}$ 可简单记成 $\alpha^{\sigma-1}$. 令 $\beta=\alpha^{-1}$, 则 $\alpha^{\sigma-1}$ 又可写成 $\alpha^{\sigma-1}=\alpha^{\sigma}/\alpha=\beta/\beta^{\sigma}=\beta^{1-\sigma}$.

引理 3 *B 是 Z 的一个子群，而且 $B\cong K^*/F^*$.*

证明 首先每个 η_α 是一个叉同态. 因为

$$\eta_\alpha(\sigma\tau)=\frac{\alpha^{\sigma\tau}}{\alpha}=\frac{\alpha^{\sigma}}{\alpha}\cdot\frac{\alpha^{\sigma\tau}}{\alpha^{\sigma}}=\eta_\alpha(\sigma)\cdot\left(\frac{\alpha^{\tau}}{\alpha}\right)^{\sigma}=\eta_\alpha(\sigma)\cdot\eta_\alpha(\tau)^{\sigma}.$$

再 $\eta_\alpha\cdot\eta_\beta(\alpha)=\frac{\alpha^\sigma}{\alpha}\cdot\frac{\beta^\sigma}{\beta}=\frac{(\alpha\beta)^\sigma}{\alpha\beta}=\eta_{\alpha\beta}(\alpha)$. B 对运算封闭. 且 $\eta_\alpha\cdot\eta_{\alpha^{-1}}(\alpha)=\frac{\alpha^\sigma}{\alpha}\cdot\frac{\alpha^{-\sigma}}{\alpha^{-1}}=1=\eta_{\alpha^{-1}}\cdot\eta_\alpha(\alpha)$. 因而 η_α 的逆 $\eta_{\alpha^{-1}}\in B$. 所以 B 是 Z 的一个子群. 由 $\eta_\alpha\cdot\eta_\beta=\eta_{\alpha\beta}$ 可知映射 $K^*\to B$ 是一个同态. $\eta_\alpha=1$ 当且仅当 $\alpha^\sigma=\alpha$ 对所有 $\sigma\in G$, 即当且仅当 $\alpha\in F^*$. 所以 $K^*/F^*\cong B$. □

Z 显然是交换群. 商群 Z/B 叫做伽罗瓦群 G 对乘法群 K^* 的 **第一个上同调群**. 记作 $H^1(G,K^*)$.

定理 22 设 K/F 为一个有限伽罗瓦扩张, $G=\mathrm{Gal}(K/F)$. 若映射 $\eta:G\to K^*$ 满足诺特方程

$$\eta(\sigma\tau)=\eta(\sigma)\eta(\tau)^\sigma,\quad \sigma,\tau\in G,$$

则存在一个元素 $\gamma\in K^*$ 使得

$$\eta(\sigma)=\gamma^{\sigma-1},\quad \sigma\in G.$$

即 $\eta\in B$. 从而 $B=Z, H^1(G,K^*)=1$.

证明 根据本章 §1 引理 2,G 的元素在 K 上线性无关. 因而 $\sum\limits_{\tau\in G}\eta(\tau)\tau$ 不是 K 到自身的零映射. 因而存在一个元素 $\alpha\in K^*$ 使得

$$\beta=\left(\sum_{\tau\in G}\eta(\tau)\tau\right)(\alpha)\neq 0. \tag{2}$$

用 $\sigma\in G$ 作用于上式两端

$$\begin{aligned}\beta^\sigma&=\sigma\left[\left(\sum_{\tau\in G}\eta(\tau)\tau\right)(\alpha)\right]=\sigma\left[\sum_{\tau\in G}\eta(\tau)\tau(\alpha)\right]\\&=\sum_{\tau\in G}\eta(\tau)^\sigma\sigma\tau(\alpha)=\eta(\sigma)^{-1}\sum_{\tau\in G}\eta(\sigma)\eta(\tau)^\sigma\sigma\tau(\alpha).\end{aligned}$$

因为 $\eta(\sigma)$ 是叉同态, 有

$$\beta^\sigma=\eta(\alpha)^{-1}\sum_{\tau\in G}\eta(\sigma\tau)\sigma\tau(\alpha)=\eta(\sigma)^{-1}\sum_{\rho\in G}\eta(\rho)\rho(\alpha)=\eta(\sigma)^{-1}\beta.$$

即 $\eta(\sigma)=\beta/\beta^\sigma$, 令 $\gamma=\beta^{-1}$, 则 $\eta(\sigma)=\frac{\gamma^\sigma}{\gamma}$,$\eta\in B$, 所以 $B=Z$, 从而 $H^1(G,K^*)=1$. □

从定理 22 推得下列著名的

定理 23 (希尔伯特定理 90) 设 K/F 为一个 n 次循环扩张, $G=\mathrm{Gal}(K/F)=\langle\sigma\rangle$. 对于 $\alpha\in K^*, N_F^K(\alpha)=1$ 的充要条件是存在一个 $\beta\in K^*$ 使得

$$\alpha=\beta^{1-\sigma}.$$

证明 证充分性. 设 $\alpha=\beta^{1-\sigma}$, 于是

$$\begin{aligned}N_F^K(\alpha)&=\frac{\beta}{\beta^\sigma}\left(\frac{\beta}{\beta^\sigma}\right)^\sigma\cdots\left(\frac{\beta}{\beta^\sigma}\right)^{\sigma^{n-1}}\\&=\frac{\beta\cdot\beta^\sigma\cdots\beta^{\sigma^{n-1}}}{\beta^\sigma\cdot\beta^{\sigma^2}\cdots\beta^{\sigma^n}}\quad(\text{注意 }\sigma^n=1)\\&=\frac{N_F^K(\alpha)}{N_F^K(\alpha)}=1.\end{aligned}$$

反之, 设 $N_F^K(\alpha)=1$, 首先定义映射 $\eta:G\to K^*$ 如下:

$$\begin{aligned}&\eta(\sigma^i)=\alpha\cdot\alpha^\sigma\cdots\alpha^{\sigma^{i-1}},\quad i=1,2,\cdots\\&\eta(1)=1.\end{aligned}$$

定义是合理的, 因为当 $\sigma^n=\sigma^0=1$ 时, $\eta(\sigma^n)=\alpha\cdot\alpha^\sigma\cdots\alpha^{\sigma^{n-1}}=N_F^K(\alpha)=1=\eta(1)$. 由计算

$$\begin{aligned}\eta(\sigma^i)\eta(\sigma^j)^{\sigma^i}&=\alpha\cdot\alpha^\sigma\cdots\alpha^{\sigma^{i-1}}(\alpha\cdot\alpha^\sigma\cdots\alpha^{\sigma^{j-1}})^{\sigma^i}\\&=\alpha\cdot\alpha^\sigma\cdots\alpha^{\sigma^{i-1}}\cdot\alpha^{\sigma^i}\alpha^{\sigma^{i+1}}\cdots\alpha^{\sigma^{j+i-1}}\\&=\eta(\sigma^{i+j})=\eta(\sigma^i\cdot\sigma^j).\end{aligned}$$

因而 η 是一个叉同态. 根据定理 22, 存在一个 $\beta\in K^*$ 使得 $\eta(\sigma^i)=\beta^{1-\sigma^i}$, 特别 $\alpha=\eta(\sigma)=\beta^{1-\sigma}$. □

由定理 22 已知 $G=\mathrm{Gal}(K/F)$ 到 K^* 的叉同态 η 恒可表成 $\eta(\sigma)=\alpha^{\sigma-1}$, $\alpha\in K^*,\sigma\in G$. 反之显然. 下面考虑叉同态群 Z 的一个重要子群 H, 即由所有 G 到 F^* 的同态组成的子群. 当叉同态 η 是一个同态时, 由引理 1 已知 $\eta(\sigma)\in F^*$ 对所有 $\sigma\in G$. 反之, G 到 F^* 的任一同态也是一个叉同态.

引理 4 *设 K/F 是一个 n 次伽罗瓦扩张, $G=\mathrm{Gal}(K/F)$. 如果叉同态 $\eta(\sigma)=\alpha^{\sigma-1}$ 是一个同态, 设 η 在群 Z 内的阶为 m, 则 $F(\alpha)$ 是 F 上的一个 m 次单根式扩张, $\alpha^m=a\in F^*$.*

证明 因为叉同态 η 是一个同态, 根据引理 1, 每个 $\eta(\sigma),\sigma\in G$, 属于 F, 而且 $\eta(\sigma^n)=\eta(\sigma)^n=\eta(1)=1$. 因而 $\eta(\sigma)$ 是 F 内一个单位根, 记成 ζ_σ, 于是 $\alpha^\sigma=\zeta_\sigma\alpha$, 由于 $\eta^i(\sigma)=\zeta_\sigma^i$ 而且 η 的阶 $=m$, ζ_σ 中必有一个本原的 m 次单位根, 记为 ζ_τ. 于是 $\alpha^\tau=\zeta_\tau\alpha$, 由此可知 $\alpha,\zeta_\tau\alpha,\cdots,\zeta_\tau^{m-1}\alpha$ 在 G 下成一传递集. 因而 α 是一个 m 次元素, $[F(\alpha):F]=m$(§1 引理 4), 其次, 又因 $\eta^m(\sigma)=(\alpha^m)^{\sigma-1}=1$, 有 $(\alpha^m)^\sigma=\alpha^m$ 对所有 $\sigma\in G$, 所以 $\alpha^m=a\in F^*$. □

现在要问 Z 的子群 H 有多大? 这需要由 K/F 的伽罗瓦群和基域 F 是否包含足够多的单位根所决定.

定理 24 假设基域 F 包含一个本原的 n 次单位根 ζ, (当 $\chi(F)$ 为素数时, 从而推出 $\chi(F)$ 与 n 互素) 设 K/F 为一个 n 次循环扩张, $G = \mathrm{Gal}(K/F) = \langle\sigma\rangle$. 则 K/F 是一个单根式扩张: $K = F(\alpha), \alpha^n = a \in F^*$.

证明 定义 G 到 K^* 的映射 η 为

$$\eta(\sigma^i) = \zeta^i, \quad i = 0, 1, \cdots, n-1.$$

显然 η 是一个同态 $G \to F^*$, 因而是 G 到 K^* 的一个叉同态, 由定理 22, 存在一个 $\alpha \in K^*$ 使得

$$\eta(\sigma^i) = \alpha^{\sigma^i - 1}.$$

根据 §1 引理 4,$[F(\alpha) : F] = n$ 而且 $\alpha^n = a \in F^*$(因为 η 的阶 $= n$). □

定理 24 是定理 10 的一个推广. 而且用现在的 $\eta(\sigma^i)$ 作出的 (2) 就是拉格朗日预解式. 下一节将看到定理 24 将进一步推广成库默尔扩张.

现在再考察诺特方程的加法形式. 从而导出上述诸定理的加法形式.

设 K/F 为一个伽罗瓦扩张, $G = \mathrm{Gal}(K/F)$. 如果映射 $\eta : G \to K$ 满足

$$\eta(\sigma\tau) = \eta(\sigma) + \eta(\tau)^\sigma, \quad \sigma, \tau \in G. \tag{3}$$

则说 η **满足诺特方程 (加法形式)**, 而且称映射 η 是 G 到加法群 K 的一个 **叉同态**.

和乘法的叉同态群一样, G 到加法群 K 的叉同态全体, 按函数的加法 $\xi \cdot \eta(\sigma) = \xi(\sigma) + \eta(\sigma)$ 形成一群, 仍记作 Z. 对每个 $\alpha \in K$, 映射 $\sigma \mapsto (\sigma - 1)(\alpha) = \sigma(\alpha) - \alpha$ 是 G 到加法群 K 的一个叉同态, 仍记作 η_α, 集合 $B = \{\eta_\alpha \mid \alpha \in K\}$ 是 Z 的一个子群, 而且商群 Z/B 叫做 G **对加法群 K 的第一个上同调解**, 记作 $H^1(G, K^+)$, η_α 是一个零同态当且仅当 $(\sigma - 1)(\alpha) = 0$ 即 $\sigma(\alpha) = \alpha$, 对所有 $\sigma \in G$. 因而 η_α 是一个零同态当且仅当 $\alpha \in F$. 所以 $B \cong K^+/F^+, K^+, F^+$ 表示加法群. 同样有, 一个 G 到 K^+ 的叉同态 η 是一个同态当且仅当 $\eta(\sigma) \in F$ 对所有 $\sigma \in G$, 即 η 是一个 G 到 F^+ 的同态.

定理 25 设 K/F 为一个有限伽罗瓦扩张, $G = \mathrm{Gal}(K/F)$. 若映射 $\eta : G \to K^+$ 满足诺特方程

$$\eta(\sigma\tau) = \eta(\sigma) + \eta(\tau)^\sigma, \quad \sigma, \tau \in G,$$

于是存在一个 $\beta \in K$ 使得

$$\eta(\sigma) = (1 - \sigma)(\beta).$$

即 $\eta \in B$, 从而 $B = Z, H^1(G, K^+) = 0$.

证明 因为 K/F 是有限可分扩张，根据第七章 §9 引理 2, 存在一个 $\gamma \in K$ 使得 $T_F^K(\gamma) \neq 0$. $T_F^K(\gamma)$ 简记作 $T(\gamma)$, 于是取

$$\beta = T(\gamma)^{-1}\left(\sum_{\tau \in G} \eta(\tau)\tau\right)(\gamma),$$

用 $\sigma \in G$ 作用于上式

$$\begin{aligned}\beta^{\sigma} &= T(\gamma)^{-1}\sigma(\textstyle\sum \eta(\tau)\tau(\gamma))\\ &= T(\gamma)^{-1}(\textstyle\sum \eta(\tau)^{\sigma}\sigma\tau(\gamma))\\ &= T(\gamma)^{-1}(\textstyle\sum(\eta(\sigma\tau) - \eta(\sigma))\sigma\tau(\gamma))\\ &= T(\gamma)^{-1}\sum_{\tau \in G}\eta(\sigma\tau)\sigma\tau(\gamma) - T(\gamma)^{-1}\sum_{\tau \in G}\eta(\sigma)\sigma\tau(\gamma)\\ &= T(\gamma)^{-1}\left(\sum_{\rho \in G}\eta(\rho)\rho\right)(\gamma) - \eta(\sigma)T(\gamma)^{-1}\sum_{\tau \in G}\sigma\tau(\gamma)\\ &= \beta - \eta(\sigma)T(\gamma)^{-1}T(\gamma) = \beta - \eta(\sigma),\end{aligned}$$

所以 $\eta(\sigma) = \beta - \beta^{\sigma} = (1-\sigma)(\beta)$. 从而 $\eta \in B$. $B = Z$. $H^1(G, K^+) = 0$. □

与希尔伯特定理 90 平行的有

定理 26 设 K/F 为一 n 次循环扩张，$G = \mathrm{Gal}(K/F) = \langle\sigma\rangle$. 对于 $\sigma \in K$, $T_F^K(\alpha) = 0$ 的充要条件是存在一个 $\beta \in K$ 使得

$$\alpha = (1-\sigma)(\beta).$$

证明 充分性显然 (如定理 23 之证明), 现证必要性. 设 $T(\alpha) = T_F^K(\alpha) = 0$. 作映射 $G \to K$

$$\begin{aligned}&\eta(\sigma^i) = \alpha + \sigma(\alpha) + \cdots + \sigma^{i-1}(\alpha), \quad i = 1, 2, 3, \cdots\\ &\eta(1) = 0.\end{aligned}$$

首先定义是合理的. 因为, 当 $\sigma^n = \sigma^0 = 1$ 时有 $\eta(\sigma^n) = \alpha + \sigma(\alpha) + \cdots + \sigma^{n-1}(\alpha) - T(\alpha) = 0 = \eta(1)$. 其次 η 是一个叉同态

$$\begin{aligned}\eta(\sigma^i)\eta(\sigma^j)^{\sigma^i} &= \alpha + \sigma(\alpha) + \cdots + \sigma^{i-1}(\alpha) + [\alpha + \sigma(\alpha) + \cdots + \sigma^{j-1}(\alpha)]^{\sigma^i}\\ &= \alpha + \sigma(\alpha) + \cdots + \sigma^{i-1}(\alpha) + \sigma^i(\alpha) + \cdots + \sigma^{i+j-1}(\alpha)\\ &= \eta(\sigma^{i+j}) = \eta(\sigma^i \cdot \sigma^j).\end{aligned}$$

根据定理 25, 存在一个 $\beta \in K$ 使得 $\eta(\sigma^i) = (1-\sigma^i)(\beta)$. 特别 $\eta(\sigma) = \alpha = (1-\sigma)(\beta)$. □

定理 27 假设域 F 的特征为素数 p, 则 F 上任一 p 次循环扩张 K/F 有一个本原元素 α, 它是方程

$$x^p - x - a,\ \ a \in F$$

的根.

证明 因为 $\chi(F) = p$, 作 F 的单位元素 1 的迹 $T(1) = T_F^K(1) = 1+1+\cdots+1 = p = 0$. 应用前定理, 存在一个 $\beta \in K$ 使得 $1 = (1-\sigma)(\beta)$, 即 $\sigma(\beta) = \beta - 1$. 从而 $\sigma^i(\beta) = \beta - i$, 即 $\beta, \beta+1, \cdots, \beta+(p-1)$ 在 G 下成一传递集, β 是 F 上一个 p 次不可约多项式的根 (本章 §1 引理 4), 所以 $[F(\beta):F] = p, K = F(\beta)$. 具体算出 β 的极小多项式, 令 $\beta^p - \beta = a$. 用 σ 作用得

$$\begin{aligned} a^\sigma &= (\beta^p - \beta)^\sigma = \sigma(\beta)^p - \sigma(\beta) \\ &= (\beta-1)^p - (\beta-1) \\ &= \beta^p - 1 - (\beta - 1) = \beta^p - \beta = a. \end{aligned}$$

根据伽罗瓦扩张的定义, $a \in F$, 所以 $x^p - x - a$ 是 β 的极小多项式. □

定理 27 中的循环扩张是首先由阿廷和施赖尔 (Schreier) 作出的.

§9 库默尔理论

本节将推广前一节的定理 24 和定理 27, 以回答定理 24 前面提出的问题, 就是说如何使得一个有限伽罗瓦扩张 K/F, $G = \mathrm{Gal}(K/F)$, 的叉同态群 Z 包含足够多的同态?

定义 11 如果一个有限阿贝尔群的元素的阶的最小公倍数为 m, 则 m 叫做这群的 **指数**. 假设基域 F 包含 m 个不同的 m 次单位根 (这就自然要求当 $\chi(F)$ 为素数时 $\chi(F)$ 与 m 互素), 如果 F 上一个有限阿贝尔扩张 K/F 的伽罗瓦群 G 的指数 m' 整除 m, 则 K/F 叫做一个 **库默尔(Kummer) m-扩张**.

对于一个库默尔 m- 扩张 K/F, 它将为我们提供足够多的 G 到乘法群 F^* 的同态. 下面将立即会看到这一点.

暂时离开伽罗瓦扩张来讨论有限阿贝尔群的特征标. 设 G 为任一指数为 m' 的有限阿贝尔群, 又设域 F 包含 m 个不同的单位根. 依照群论的习惯, G 到 F^* 的任一个同态叫做 G 到 F^* 的一个 **特征标**, 用 χ 表示特征标. 当 $\chi(\sigma) = 1$ 对所有 $\sigma \in G$, 则 χ 叫做 **单位特征标**, 或 **主特征标**, 记作 $\chi = 1$. 设 χ_1, χ_2 为 G 到 F^* 的两个特征标. 它们的乘积定义为

$$\chi_1 \cdot \chi_2(\sigma) = \chi_1(\sigma) \cdot \chi_2(\sigma),\ \ \sigma \in G.$$

χ_1 的逆定义为

$$\chi_1^{-1}(\sigma) = \chi_1(\sigma)^{-1}, \quad \sigma \in G.$$

从 §8 已知，$\chi_1 \cdot \chi_2$ 和 χ_1^{-1} 仍为特征标. 因而 G 到 F^* 的特征标全体成一群，它叫做 G 的 **特征标群**, 记作 $\hat{G}$. 单位特征标就是 $\hat{G}$ 的单位元素. 为了得到足够多的特征标，以下恒假定 G 的指数 m' 整除 m.

引理 1 *设域 F 包含 m 个不同的单位根，又设 G 为一个有限阿贝尔群，其指数 m' 整除 m, 于是 G 到 F^* 的特征标群 $\hat{G}$ 有如下的性质:*

1) $\hat{G} \cong G$;

2) $\bigcap_{\chi \in \hat{G}} \ker(\chi) = \{1\}$.

证明

1) 根据第六章可知，一个有限阿贝尔群可以写成循环子群的直积，设 G 已表成它的循环子群 $G_i, i = 1, \cdots, r$ 的直积

$$G = G_1 \times G_2 \times \cdots \times G_r,$$

而且 $G_i = \langle \sigma_i \rangle$, σ_i 的阶 $= m_i$, $i = 1, \cdots, r$. G 的每个元素 σ 可以唯一地表成

$$\sigma = \sigma_1^{\nu_1} \sigma_2^{\nu_2} \cdots \sigma_r^{\nu_r}, \quad 0 \le \nu_i < m_i. \tag{1}$$

由 $m_i | m'$, 有 $m_i | m$. 根据对 F 的假设，F 含有本原的 m_i 次单位根，注意取定一个本原的 m_i 次单位根 ζ_i. 定义 G 到 F^* 的特征标 χ_i 如下

$$\chi_i(\sigma) = \zeta_i^{\nu_i}, \quad i = 1, \cdots, r.$$

显然，χ_i 是一个特征标，其次 χ_i 的阶 $= m_i$. 因为 $\chi_i^{m_i}(\sigma) = \zeta_i^{\nu_i m_i} = 1$ 对所有 $\sigma \in G$, 因而 $\chi_i^{m_i} = 1$. 而且若 $\chi_i^k = 1$, 则 $\chi_i^k(\sigma_i) = (\zeta_i)^k = 1$, 从而 $m_i | k$, 所以 χ_i 的阶 $= m_i$. 其次证明 $\chi_1, \cdots, \chi_r$ 是独立的，设有 $\chi_1^{k_1} \chi_2^{k_2} \cdots \chi_r^{k_r} = 1$. 于是等式对 σ_i 作用得

$$\chi_1^{k_1} \cdot \chi_2^{k_2} \cdots \chi_r^{k_r}(\sigma_i) = 1.$$

左端等于 $\chi_1^{k_1}(\sigma_i)\chi_2^{k_2}(\sigma_i) \cdots \chi_r^{k_r}(\sigma_i) = \chi_i^{k_i}(\sigma_i) = \zeta_i^{k_i}$, 从而 $\zeta_i^{k_i} = 1, m_i | k_i$. 由此可知每个乘积项 $\chi_i^{k_i} = 1$. 所以 $\chi_1, \cdots, \chi_r$ 是独立的. 最后证明 G 到 F^* 的每个特征标 χ 可表成 $\chi_1, \cdots, \chi_r$ 的方幂的乘积. 我们知道，χ 将 σ_i 映到一个 m_i 次单位根，因而 $\chi(\sigma_i) = \zeta_i^{k_i}$. 于是

$$\begin{aligned}\chi(\sigma) &= \prod_{i=1}^{r} \chi(\sigma_i^{\nu_i}) = \prod_{i=1}^{r} \zeta_i^{\nu_i k_i} = \prod_{i=1}^{r} \chi_i^{k_i}(\sigma_i^{\nu_i}) \\ &= \prod_{i=1}^{r} \chi_i^{k_i}(\sigma) = \left(\prod_{i=1}^{r} \chi_i^{k_i}\right)(\sigma), \quad \text{对所有的} \sigma \in G.\end{aligned}$$

所以 $\chi = \chi_1^{k_1}\chi_2^{k_2}\cdots\chi_r^{k_r}$. 令 $\hat{G}_i = \langle\chi_i\rangle$, 于是 $\hat{G}$ 是循环子群 $\hat{G}_i$ 的直积, 且 $|\hat{G}_i| = m_i$. 最后得 $G \cong \hat{G}$.

2) 设 $\sigma \in \bigcap\limits_{\chi\in\hat{G}} \ker(\chi)$, 将 σ 表为 (1) 式, 作用 χ_i 于 σ 得 $1 = \chi_i(\sigma) = \zeta_i^{\nu_i}$, 从而 $m_i|\nu_i$, $i = 1,\cdots,r$. $\sigma = 1$. 所以 $\bigcap\limits_{\chi\in\hat{G}} \ker(\chi) = \{1\}$. □

由引理 1 我们已经知道有限阿贝尔群 G 和它的特征标群 $\hat{G}$ 同构. 我们可以继续求 $\hat{G}$ 的特征标群 $\hat{\hat{G}}$, 当然它们三者是同构的, 好像得不出什么新东西. 但是值得推敲的是我们可以按自然的方式来建立 G 与 $\hat{\hat{G}}$ 之间的同构映射. 我们将 G 的特征标 $\chi(\sigma)$ 写成对称的形式

$$\chi(\sigma) = (\chi,\sigma),$$

(χ,σ) 适合运算规律

$$(\chi_1\cdot\chi_2,\sigma) = (\chi_1,\sigma)\cdot(\chi_2,\sigma), \tag{2}$$

和

$$(\chi,\sigma\tau) = (\chi,\sigma)\cdot(\chi,\tau). \tag{3}$$

(3) 表示 χ 是 G 到 F^* 的一个特征标, 而 (2) 则表示 σ 确定了 $\hat{G}$ 到 F^* 的一个特征标, 记作 $\hat{\sigma}$. 用函数的符号写出就是

$$\hat{\sigma}(\chi) = \chi(\sigma).$$

由计算,

$$\widehat{\sigma\tau}(\chi) = \chi(\sigma\tau) = \chi(\sigma)\cdot\chi(\tau) = \hat{\sigma}(\chi)\cdot\hat{\tau}(\chi) = \hat{\sigma}\cdot\hat{\tau}(\chi)$$

对所有的 $\chi \in \hat{G}$ 都成立, 因而 $\widehat{\sigma\tau} = \hat{\sigma}\cdot\hat{\tau}$. 这表明映射 $\sigma \mapsto \hat{\sigma}$ 是 G 到 $\hat{\hat{G}}$ 的一个同态. 它是单射的, 因为, 若 $\hat{\sigma} = \hat{\tau}$, 则 $\hat{\sigma}(\chi) = \hat{\tau}(\chi)$ 对所有 $\chi \in \hat{G}$, 从而 $\chi(\sigma) = \chi(\tau)$, $\chi(\sigma\tau^{-1}) = 1$ 对所有的 $\chi \in \hat{G}$. 于是 $\sigma\tau^{-1} \in \bigcap\limits_{\chi\in\hat{G}} \ker(\chi)$. 由引理 1 知 $\sigma\tau^{-1} = 1, \sigma = \tau$. 于是得到

引理 2 F, G 假设如引理 1, 每个 $\sigma \in G$ 定义了 $\hat{G}$ 的一个特征标 $\hat{\sigma}$ 如下

$$\hat{\sigma}(\chi) = \chi(\sigma),\ \ \chi \in \hat{G}$$

于是映射 $\sigma \mapsto \hat{\sigma}$ 给出了 G 到 $\hat{\hat{G}}$ 的一个标准同构.

推论 若 $\hat{G}$ 的子群 $\hat{H}$ 满足 $\bigcap\limits_{\chi\in\hat{H}} \ker(\chi) = \{1\}$, 则 $\hat{H} = \hat{G}$.

证明 G 的阶记作 n. 对不同的 $\sigma, \tau \in G$, 我们说 $\hat{\sigma}$ 和 $\hat{\tau}$ 在 $\hat{H}$ 上的限制也不同. 假若在 $\hat{H}$ 上 $\hat{\sigma} = \hat{\tau}$. 于是 $\hat{\sigma}(\chi) = \hat{\tau}(\chi)$ 对所有 $\chi \in \hat{H}$ 成立. 即 $\chi(\sigma) = \chi(\tau)$

从而 $\chi(\sigma\tau^{-1})=1$ 对所有 $\chi\in\hat{H}$ 成立. 因而 $\sigma\tau^{-1}\in\bigcap_{\chi\in\hat{H}}\ker(\chi)$. 即 $\sigma\tau^{-1}\in\{1\}$. 将有 $\sigma\tau^{-1}=1,\sigma=\tau$. 这不可能. 因此将所有 $\hat{\sigma}$ 限制在 $\hat{H}$ 上就得 $\hat{H}$ 的 n 个不同的特征标. 由引理 1 可知 $|\hat{H}|\geq n$. 另一方面 $\hat{H}\subset\hat{G}$, 又有 $|\hat{H}|\leq|\hat{G}|=n$. 所以 $|\hat{H}|=n$, 从而 $\hat{H}=\hat{G}$. □

下面来讨论库默尔扩张. 设基域 F 包含 m 个不同的 m 次单位根, K/F 为一个有限的库默尔 m- 扩张, $G=\mathrm{Gal}(K/F),\hat{G}$ 为 G 的特征标群. 对于每个 $\chi\in\hat{G}$, 根据定理 22, 存在一个 $\theta_\chi\in K^*$ 使得

$$\chi(\sigma)=\theta_\chi^{\sigma-1},\quad \sigma\in G, \tag{4}$$

因为 K/F 是一个库默尔 m- 扩张, G 以及 $\hat{G}$ 的指数 m' 整除 m. 因而 $\chi^m=1$. 根据 §8 引理 4 可知, 适合 (4) 的任一个 θ_χ, 它的 m 次方属于 F^*. 将会立即看到反过来也对. 这样我们在 K^* 内定义一个子群 M_K 如下

$$M_K=\{\theta\in K^*\,|\,\theta^m\in F^*\}.$$

显然 $F^*\subset M_K$, 而且 M_K 包含 (4) 的一切解 $\theta_\chi,\chi\in\hat{G}$. 与 (4) 相反, 我们来建立一个映射 $\eta:M_K\to\hat{G}$: 对每个 $\theta\in M_K$, 有 $\theta^m=a\in F^*$, 对任何一个 $\sigma\in G,\theta^\sigma$ 与 θ 一样适合 χ^m-a. 因而 $\theta^\sigma=\zeta_\sigma\theta$. ζ_σ 为一个 m 次单位根. 由假设 $\zeta_\sigma\in F^*$ 对所有 $\sigma\in G$. 因此映射 $\sigma\mapsto\theta^{\sigma-1}=\zeta_\sigma$ 不仅是 G 到 K^* 的一个叉同态而且是 G 到 F^* 的一个特征标, 记作 χ_θ. χ_θ 由

$$\chi_\theta(\sigma)=\theta^{\sigma-1},\quad \theta\in M_K \tag{5}$$

所定义, 而且 $\eta(\theta)=\chi_\theta$ 是 M_K 到 $\hat{G}$ 的一个满同态. 核 $\ker(\eta)=F^*$. 这就证明了下列引理的第一部分

引理 3 M_K 定义如上. 于是

1) $M_K/F^*\cong\hat{G}$, 这个同构可由用 (5) 规定的映射 $\eta:\theta\mapsto\chi_\theta$ 来实现, $\ker(\eta)=F^*$.

2) 若 $\chi_1,\cdots,\chi_r$ 生成 $\hat{G}$, 则由 (4) 规定的 $\theta_{\chi_1},\cdots,\theta_{\chi_r}$ 为代表的陪集生成 M_K/F^*, 即 $\theta_{\chi_1},\cdots,\theta_{\chi_r}$ 和 F^* 生成 M_K.

3) 令 $N_K=\{\theta^m\,|\,\theta\in M_K\}$ 即 M_K^m, 于是

$$M_K/F^*\cong N_K/F^{*m}.$$

这个同构可由幂映射 $\lambda:\theta\mapsto\theta^m,\theta\in M_K$ 来实现.

证明

1) 已经证明在上面.

2) 由 1) 即得.

3) 映射 $\lambda: M_K \to N_K$ 显然是一个满同态, 而且 λ 将 F^* 映到 F^{*m} 上. 现在只需证 $\lambda^{-1}(F^{*m}) = F^*$. 已有 $F^* \subset \lambda^{-1}(F^{*m})$. 反之, 设 $\alpha \in \lambda^{-1}(F^{*m})$, 于是 $\alpha^m = b \in F^{*m}$. 存在一个 $a \in F^*$ 使得 $b = a^m$. 于是 $\left(\frac{\alpha}{a}\right)^m = 1, \frac{\alpha}{a} = \zeta$ 是一个 m 次单位根. 由假设 $\zeta \in F^*$ 因而 $\alpha = \zeta a \in F^*$. 所以 $F^* = \lambda^{-1}(F^{*m})$. 由此即得 3). □

对于每个 $a \in N_K$, 多项式 $x^m - a$ 的根可写成 $\sqrt[m]{a}, \zeta_1 \sqrt[m]{a}, \cdots, \zeta_{m-1} \sqrt[m]{a}$, 其中 $\sqrt[m]{a}$ 是 $x^m - a$ 的任一根, 而 $\{1, \zeta_1, \cdots, \zeta_{m-1}\}$ 是 F 的 m 个不同的 m 次单位根. 用 $N_K^{\frac{1}{m}}$ 表示所有多项式 $x^m - a, a \in N_K$ 的根的全体. 由于 $M_K^m = N_K$ 而且 $\{1, \zeta_1, \cdots, \zeta_{m-1}\} \subset M_K$, 我们有 $N_K^{\frac{1}{m}} = M_K$.

定理 28 设基域 F 包含 m 个不同的 m 次单位根, K/F 为一个有限库默尔 m- 扩张, $G = \mathrm{Gal}(K/F)$, 而且 $\hat{G}, M_K, N_K$ 定义如下. 于是

1) $K = F(M_K)$ 或 $K = F(N_K^{\frac{1}{m}})$. 更精确地说, 若特征标 $\chi_1, \cdots, \chi_r$ 生成 $\hat{G}$, 则由 (4) 定义的 $\theta_{\chi_1}, \cdots, \theta_{\chi_r}$ 在 F 上生成 K 即 $K = F(\theta_{\chi_1}, \cdots, \theta_{\chi_r})$. 反之也对.

2) $\hat{G} \cong N_K / F^{*m}$.

证明

1) 设 $\chi_1, \cdots, \chi_r$ 生成 $\hat{G}$, 求证 $K = F(\theta_{\chi_1}, \cdots, \theta_{\chi_r})$. 设 $\sigma \in G$ 为任一元使得 σ 保持每个 θ_{χ_i} 不动. 于是 $\chi_i(\sigma) = \theta_{\chi_i}^{\sigma - 1} = 1$, 对 $i = 1, \cdots, r$. 因为 $\chi_1, \cdots, \chi_r$ 生成 $\hat{G}$, 每个 $\chi \in \hat{G}$ 可表成 $\chi = \chi_1^{e_1} \cdots \chi_r^{e_r}$. 于是 $\chi(\sigma) = \prod_{i=1}^{r} \chi_i(\sigma)^{e_i} = 1$, 从而 $\sigma \in \bigcap_{\chi \in \hat{G}} \ker(\chi)$. 根据引理 1, 得 $\sigma = 1$, 根据伽罗瓦基本定理, $F(\theta_{\chi_1}, \cdots, \theta_{\chi_r}) = K$.

2) 由引理 3 即得. □

定理 29 设基域 F 包含 m 个不同的 m 次单位根. 设 N 为乘法群 F^* 的一个子群, $F^{*m} \subset N$ 而且 $[N : F^{*m}]$ 有限, 用 $N^{\frac{1}{m}}$ 表示所有多项式 $x^m - a$, $a \in N$, 的根的全体. 将 $N^{\frac{1}{m}}$ 添加到 F 得到扩域 $K = F(N^{\frac{1}{m}})$, 则 K/F 是一个有限的库默尔 m- 扩张. 而且由 $G = \mathrm{Gal}(K/F)$ 的特征标群 $\hat{G}$ 所决定的 $M_K = N^{\frac{1}{m}}$.

证明 对每个多项式 $x^m - a, a \in N$, 任意取定它的一个根, 记作 $\sqrt[m]{a}$ 将 $S = \{\sqrt[m]{a} \mid a \in N\}$ 添加到 F 得的扩域 $F(\{\sqrt[m]{a} \mid a \in N\})$, 由于 F 包含 m 个不同的 m 次单位根, 它包含每个 $x^m - a$ 的全部根, 因而 $K = F(\{\sqrt[m]{a} \mid a \in N\})$, 而且 K/F 是可分的. 于是 K/F 是一个伽罗瓦扩张. 其次证明 $G = \mathrm{Gal}(K/F)$ 是一个交换群. 每个 $\sigma \in G$ 由它在 S 上的作用完全确定. 只需证明 K 的任意两

个 F- 自同构 σ 和 τ 在每个根式 $\sqrt[m]{a}, a \in N$, 上的作用可以交换即够. 令

$$\sigma(\sqrt[m]{a}) = \zeta^r \sqrt[m]{a}, \ \tau(\sqrt[m]{a}) = \zeta^s \sqrt[m]{a},$$

其中 ζ 是 F 中一个本原的 m 次单位根. 由计算

$$\sigma\tau(\sqrt[m]{a}) = \sigma(\tau(\sqrt[m]{a})) = \sigma(\zeta^s \sqrt[m]{a}) = \zeta^s \sigma(\sqrt[m]{a}) = \zeta^s \zeta^r \sqrt[m]{a} = \zeta^{r+s} \sqrt[m]{a}.$$

另一方面,

$$\begin{aligned}\tau\sigma(\sqrt[m]{a}) &= \tau(\sigma(\sqrt[m]{a})) = \tau(\zeta^r \sqrt[m]{a}) = \zeta^r \tau(\sqrt[m]{a}) \\ &= \zeta^r \zeta^s \sqrt[m]{a} = \zeta^{r+s} \sqrt[m]{a}.\end{aligned}$$

所以 $\sigma\tau(\sqrt[m]{a}) = \tau\sigma(\sqrt[m]{a})$ 对所有 $a \in N$. 由此推出 $\sigma\tau = \tau\sigma$. 其次, 对所有的 $a \in N$, 有

$$\sigma^m(\sqrt[m]{a}) = \sigma^{m-1}(\zeta^r \sqrt[m]{a}) = \cdots = \zeta^{rm} \cdot \sqrt[m]{a} = \sqrt[m]{a}.$$

因而 $\sigma^m = 1$. 所以 G 是一个指数整除 m 的交换群. 最后在建立映射 $\eta : N^{\frac{1}{m}} \to \hat{G}$ 以前, 需要说明 $[K : F] < \infty$. 由假设 N/F^{*m} 有限, 将 N 按 F^{*m} 分解成陪集的并 $N = a_1F^{*m} \cup \cdots \cup a_sF^{*m}$. 显而易见 $K = F(\sqrt[m]{a_1}, \cdots, \sqrt[m]{a_s})$. 从而 $[K : F] \leq m^s < \infty$. 将 $N^{\frac{1}{m}}$ 简记作 M. M 的每个元素 θ 是某个 $x^m - a$, $a \in N$ 的根. 反之, 每个 $x^m - a$, $a \in N$, 的全部根都属于 M. 而且 $F^* \subset M$. M 的每个元素 θ 定义了 G 到 K^* 的一个义同态 $\chi_\theta : \sigma \mapsto \theta^{\sigma - 1}, \sigma \in G$. 由于 θ, θ^σ 都是 $x^m - a$ 的根, $\theta^{\sigma-1}$ 是一个 m 次单位根, 属于 F^*. 因而 χ_θ 是 G 的一个特征标. 我们定义 $\eta : M \to \hat{G}$

$$\eta(\theta) = \chi_\theta,$$

η 是一个同态而且 $\ker(\eta) = F^*$. 最后证明 η 是满射. 令 $\eta(M) = \hat{H}$, $\hat{H}$ 是 $\hat{G}$ 的一个子群. 为了证明 $\hat{H} = \hat{G}$. 首先指出 $\bigcap\limits_{\chi \in \hat{H}} \ker(\chi) = \{1\}$. 设 $\sigma \in G$ 为任一元素使得 $\chi_\theta(\sigma) = 1$ 对所有 $\theta \in M$, 于是对所有 $\theta \in M$ 有 $\theta^\sigma = \theta$. 这表明 σ 是 K 的恒等自同构, $\sigma = 1$. 因而 $\bigcap\limits_{\chi \in \hat{H}} \ker(\chi) = \{1\}$. 根据引理 2 的推论, $\hat{H} = \hat{G}$. 所以 η 是 M 到 $\hat{G}$ 的一个满同态, 而且 $\ker(\eta) = F^*$. 同时也证明了, 当 $\chi_1, \cdots, \chi_r$ 生成 $\hat{G}$ 时, 由 (4) 规定的 $\theta_{\chi_1}, \cdots, \theta_{\chi_r}$ 和 F^* 生成 M. 现在的 M 就是引理 3 中的 M_K, 因而 $N^{\frac{1}{m}} = M_K$. □

说明 在定理 29 中, 在乘法群 N 中取一组元素 $a_1, \cdots, a_r$ 使得以 a_i 为代表的陪集 $\bar{a}_1, \cdots, \bar{a}_r$ 是 N/F^{*m} 的一组独立生成元. 令 $\sqrt[m]{a_i}$ 表示 $x^m - a_i$ 的任一根. 则 $K = F(\sqrt[m]{a_1}, \cdots, \sqrt[m]{a_r})$. 设 $\bar{a}_i$ 的阶为 m_i, $i = 1, \cdots, r$. 于是 $a_i^{m_i} \in F^{*m}$, $a_i^{m_i}$ 可表成 b_i^m, $b_i \in F^*$. 令 $m = m_i q_i$, $i = 1, \cdots, r$. 于是 $a_i = \zeta_i b_i^{q_i}$, 其中 ζ_i 为一个

m_i 次单位根. 设 ζ 为一个本原的 m 次单位根. 于是 ζ^{q_i} 是一个本原的 m_i 次单位根, ζ_i 可表成 $\zeta_i = \zeta^{\gamma_i q_i}, a_i = (\zeta^{\nu_i} b_i)^{q_i}$. $x^m - a_i$ 在 $F[x]$ 内可分解成

$$x^m - a_i = x^m - (\zeta^{\nu_i} b_i)^{q_i} = \prod_{j=0}^{q_i-1} (x^{m_i} - \zeta^{m_i j+\nu_i} b_i),$$

$\sqrt[m]{a_i}$ 是其中一个因式的根. $\sqrt[m]{a_i}$ 是一个 m_i 次不可约根式. $\sqrt[m]{a_i}$ 可换写成 $\sqrt[m_i]{c_i}, c_i$ 为某一个 $\zeta^{m_i j+\nu_i} b_i$. 最后 $K = F(\sqrt[m_1]{c_1}, \cdots, \sqrt[m_r]{c_r})$. $\sqrt[m_i]{c_i}$ 的陪集构成 M/F^* 的一组独立生成元.

下面将对 §8 定理 27 作一个推广. 以下恒假定基域的特征为一个素数 p. 当然 p 个元素的域 $\mathbf{F}_p$ 是它的一个子域. 设 K/F 为一个 p^n 次阿贝尔扩张, 而且 $G = \mathrm{Gal}(K/F)$ 是一个初等 p- 群, 即 G 为 $(p, p, \cdots, p)$ 型阿贝尔群. G 到加法群 $\mathbf{F}_p^+$ 的同态叫做 G 的 **特征标**, 仍用 χ, χ_1, χ_2 等表示. 于是

$$\chi(\sigma\tau) = \chi(\sigma) + \chi(\tau), \quad \sigma, \tau \in G.$$

它们的运算定义为

$$(\chi_1 + \chi_2)(\sigma) = \chi_1(\sigma) + \chi_2(\sigma).$$

这样 G 的特征标全体形成一群, 叫做 G 的 **特征标群**, 记作 $\hat{G}$.

引理 1 和引理 2 及其推论对现在的情况仍然有效.

G 的每个特征标 χ 适合加法形式的诸特方程, 根据定理 25, 存在一个 $\theta_\chi \in K$ 使得

$$\chi(\sigma) = \sigma(\theta_\chi) - \theta_\chi, \quad \sigma \in G. \tag{6}$$

对于任一元素 $a \in F, a + \theta_\chi$, 也和 θ_χ 一样满足 (6):

$$\begin{aligned}\sigma(a + \theta_\chi) - (a + \theta_\chi) &= \sigma(a) + \sigma(\theta_\chi) - a - \theta_\chi \\ &= a + \sigma(\theta_\chi) - a - \theta_\chi = \sigma(\theta_\chi) - \theta_\chi = \chi(\sigma).\end{aligned}$$

反之, 设 θ 为 K 的任一元素而且和 θ_χ 一样适合

$$\chi(\sigma) = \sigma(\theta) - \theta, \quad \sigma \in G. \tag{7}$$

(7) − (6) 得 $0 = \sigma(\theta - \theta_\chi) - (\theta - \theta_\chi)$, 从而 $\sigma(\theta - \theta_\chi) = \theta - \theta_\chi$ 对所有 $\sigma \in G$. 根据伽罗瓦扩张的定义, $\theta - \theta_\chi = a \in F$, 即 θ 属于陪集 $\theta_\chi + F$. 因而 (7) 的全部解 (对给定的 χ) 为 $\theta_\chi + F$.

其次研究 $\theta_\chi + F$ 的元素的特定. 由于 $\chi(\sigma) \in \mathbf{F}_p, \chi(\sigma)^p = \chi(\sigma)$. 将 (7) 两端升高 p 次方, 考虑到 $\chi(F) = p$, 得

$$\chi(\sigma) = \sigma(\theta^p) - \theta^p. \tag{8}$$

(8) − (7) 得 $\sigma(\theta^p-\theta)=\theta^p-\theta$ 对所有 $\sigma\in G$. 于是 $\theta^p-\theta=a\in F$. 因而 θ 是多项式

$$x^p-x-a,\ \ a\in F \tag{9}$$

的一根. 反之, 对任一 $a\in F$, 设多项式 (9) 在 K 内有一根 θ. 作

$$\chi_\theta(\sigma)=\sigma(\theta)-\theta,\ \ \sigma\in G. \tag{10}$$

χ_θ 当然是 G 到 K^+ 的一个叉同态. 不仅如此, 将 (10) 升高 p 次方, $\chi_\theta(\sigma)^p=\sigma(\theta^p)-\theta^p$, 然后与 (10) 相减得

$$\chi_\theta(\sigma)^p-\chi_\theta(\sigma)=\sigma(\theta^p-\theta)-(\theta^p-\theta)=\sigma(a)-a=0.$$

从而 $\chi_\theta(\sigma)^p=\chi_\theta(\sigma),\chi_\theta(\sigma)\in\mathbf{F}_p$ 对所有的 $\sigma\in G$. 因而 χ_θ 还是 G 的一个特征标. 总之, *由 (10) 定义的 χ_θ 是 G 的一个特征标当且仅当 θ 是方程 (9) 的一根.*

引进符号 $\mathcal{P}$, 用 $\mathcal{P}(\theta)$ 表示 $\theta^p-\theta$, $\theta\in K$. 对子集 $S\subset K$, 用 $\mathcal{P}(S)$ 表示 $\{\mathcal{P}(\theta)\,|\,\theta\in S\}$. 多项式 (9) 可记成 $\mathcal{P}(x)-a$. 用 $\mathcal{P}^{-1}(a)$ 表示多项式 (9) 在 K 内的任一根. 用 $\mathcal{P}^{-1}(S)$ 表示所有多项式 $x^p-x-a,a\in S$, 的全部根构成的集合.

令 $M_K=\{\theta\in K\,|\,\mathcal{P}(\theta)\in F\},N_K=\mathcal{P}(M_K)$. 综合上面的结果得到引理的第一部分.

引理 4 *$F,K/F,G,\hat{G},M_K,N_K$ 定义如上, 于是*

1) 对 M_K 的每个元素 θ 由 (10) 定义的 χ_θ 是 G 的一个特征标. 反之, 对 $\hat{G}$ 的每个元素 χ, (7) 的一切解 θ 属于 M_K.

2) $M_k/F^+\cong\hat{G}$. 这个同构可由 (10) 规定的映射 $\theta\mapsto\chi_\theta$ 来实现. 从而 $\chi_1,\cdots,\chi_r$ 生成 $\hat{G}$ 当而且仅当 $\theta_{\chi_1},\cdots,\theta_{\chi_r}$ 和 F^+ 生成 M_K.

3) $M_K/F^+\cong N_K/\mathcal{P}(F^-)$. 这个同构可由 $\mathcal{P}$- 映射

$$\theta\to\mathcal{P}(\theta),\ \theta\in M_K$$

来实现.

证明 1) 已证明在上面.

2) 由 (10) 规定的映射 $\eta:\theta\mapsto\chi_\theta$, 由 1) 可知是 M_K 到 $\hat{G}$ 的一个满射. 而且由 $\hat{G}$ 的运算可知 η 是一个同态. χ_θ 是 G 到 $\mathbf{F}_p$ 的一个零同态当且仅当 $\sigma(\theta)=\theta$ 对所有的 $\sigma\in G$ 即 $\theta\in F$. 因而 $\ker(\eta)=F^+$.

3) 根据 N_K 的定义, $\mathcal{P}$- 映射 $\theta\mapsto\mathcal{P}(\theta)$ 是一个满射. 而且对于 $\theta_1,\theta_2\in M_K$ 有

$$\begin{aligned}\mathcal{P}(\theta_1+\theta_2)=&(\theta_1+\theta_2)^p-(\theta_1+\theta_2)\\=&\theta_1^p+\theta_2^p-\theta_1-\theta_2\\=&\mathcal{P}(\theta_1)+\mathcal{P}(\theta_2),\end{aligned}$$

因而 $\mathcal{P}$ 是一个同态. 显然 $\mathcal{P}$ 将 F^+ 映射到 $\mathcal{P}(F^+)$, 即 $F^+ \subset \mathcal{P}^{-1}(\mathcal{P}(F^+))$. 设 $\alpha \in \mathcal{P}^{-1}(\mathcal{P}(F^+))$, 于是存在一个 $a \in F$ 使得 $\mathcal{P}(\alpha) = \mathcal{P}(a)$, 即 $\alpha^p - \alpha = a^p - a$, 移项得 $(\alpha - a)^p = \alpha - a$, 从而 $\alpha - a = b \in \mathbf{F}_p$. 由 $\mathbf{F}_p \subset F$ 可知 $\alpha = a + b \in F^+$. 所以 $\mathcal{P}^{-1}(\mathcal{P}(F^+)) = F^+$. 由此得 $M_K/F^+ \cong N_K/\mathcal{P}(F^+)$. □

定理 30 设 F 为一个素数特征 p 的域, K/F 为一个 p^n 次阿贝尔扩张, 而且 $G = \mathrm{Gal}(K/F)$ 为一个初等 p- 群. 于是

1) $K = F(M_K) = F(\mathcal{P}^{-1}(N_K))$. 更精确地说, 若 $\chi_1, \cdots, \chi_r$ 是 G 的一组生成元, 则由 (6) 规定的 $\theta_{\chi_1}, \cdots, \theta_{\chi_r}$ 在 F 上生成 $K, K = F(\theta_{\chi_1}, \cdots, \theta_{\chi_r})$.

2) $\hat{G} \cong N_K/\mathcal{P}(F^+)$.

证明 1) 设 $\chi_1, \cdots, \chi_r$ 为 $\hat{G}$ 的一组生成元, 求证 $F(\theta_{\chi_1}, \cdots, \theta_{\chi_r}) = K$. 设 σ 为 G 的任一元素使得 $\sigma(\theta_{\chi_i}) = \theta_{\chi_i}, i = 1, \cdots, r$. 于是 $\chi_i(\sigma) = 0$ 对所有 i. 由于 χ_i 生成 $\hat{G}$, $\hat{G}$ 的任一 χ 可表成 $\chi_1, \cdots, \chi_r$ 的整系数线性组合 $\chi = e_1\chi_1 + \cdots + e_r\chi_r$. 于是 $\chi(\sigma) = \sum_{i=1}^{r} e_i\chi_i(\sigma) = 0$, 从而 $\sigma \subset \bigcap_{\chi \in \hat{G}} \ker(\chi)$. 根据引理 1, $\sigma = 1$. 由伽罗瓦基本定理, $F(\theta_{\chi_1}, \cdots, \theta_{\chi_r}) = K$.

2) 由引理 4 即得. □

定理 31 设 F 为一个素数特征 p 的域. 又设 N 为加法群 F^+ 的一个子群, 包含 $\mathcal{P}(F^+)$ 而且 $[N : \mathcal{P}(F^+)]$ 有限. 将所有多项式 $\mathcal{P}(x) - a, a \in N$, 的根添加到 F 得到的扩域 K, 则

1) K 是一有限的 p^n 次阿贝尔扩张, 而且 $G = \mathrm{Gal}(K/F)$ 是一个初等 p-群.

2) $\mathcal{P}^{-1}(N)$ 等于由特征标群 $\hat{G}$ 所决定的 M_K.

证明 1) 只要添加 $\mathcal{P}(x) - a$ 的一个根 θ 到 F 得到的扩域 $F(\theta)$ 就包含 $\mathcal{P}(x) - a$ 的全部根 $\theta, \theta + 1, \cdots, \theta + p - 1$. 因而 K/F 是可分的. 在 N 内取一组元素 $a_1, \cdots, a_r$ 使得陪集 $\bar{a}_1, \cdots, \bar{a}_r$ 生成 $N/\mathcal{P}(F^+)$. 令 θ_i 为 $\mathcal{P}(x) - a_i$ 的一根. 令 $L = F(\theta_1, \cdots, \theta_r)$, N 的任一元素 a 可表成 $a = k_1a_1 + \cdots + k_ra_r + b$, $k_i \in \mathbf{F}_p$, $b \in \mathcal{P}(F^+)$, b 可表成 $b = c^p - c, c \in F$. 由计算可知 $\theta = k_1\theta_1 + \cdots + k_r\theta_r + c$ 是 $\mathcal{P}(x) - a$ 的根:

$$\begin{aligned}\theta^p - \theta =& (k_1\theta_1 + \cdots + k_r\theta_r + c)^p - (k_1\theta_1 + \cdots + k_r\theta_r + c) \\ =& k_1(\theta_1^p - \theta_1) + \cdots + k_r(\theta_r^p - \theta_r) - c^p - c \\ =& k_1a_1 + \cdots + k_ra_r + b \\ =& a.\end{aligned}$$

因此 L 也包含每个 $\mathcal{P}(x) - a$, $a \in N$, 的一根, 当然包含它的全部根. 所以 $L = K$. 这表明 K/F 是一个有限可分正规扩张. 其次证明 $G = \mathrm{Gal}(K/F)$ 是交换群. 设

σ,τ 为 G 的任意两元素，对每个 $a\in N$, 用 θ 表示 $\mathcal{P}(x)-a$ 的一个根. σ,τ 作用于 θ 分别有

$$\sigma(\theta)=\theta+j,\quad \tau(\theta)=\theta+k,\quad j,k\in\mathbf{F}_p.$$

于是

$$\sigma\tau(\theta)=\sigma(\tau(\theta))=\sigma(\theta+k)=\sigma(\theta)+k=\theta+j+k,$$

同样

$$\tau\sigma(\theta)=\tau(\sigma(\theta))=\tau(\theta+j)=\tau(\theta)+j=\theta+k+j,$$

所以 σ,τ 在 $\mathcal{P}(x)-a$ 的根上的作用是可交换的，于是 $\sigma\cdot\tau=\tau\cdot\sigma$. 这就证明了 G 是交换群. 再计算 σ 的阶.

$$\sigma^p(\theta)=\sigma^{p-1}(\theta+j)=\sigma^{p-2}(\theta+2j)=\cdots=\theta-pj=\theta.$$

σ^p 保持 $\mathcal{P}(x)-a$ 的每个根不动. 因而 $\sigma^p=1$. 这表明 $\sigma=1$ 或 σ 的阶 $=p$. 所以 G 是一个初等 p- 群.

其次证明 2). 令 M 表示所有多项式 $\mathcal{P}(x)-a$, $a\in N$, 的全部根构成的集合. 于是 $\mathcal{P}(M)=N$, 而且 $F\subset M$. 对每个 $\theta\in M$, 利用 (7) 定义了 G 到 K^+ 的一个叉同态 χ_θ 即 $\chi_\theta(\sigma)=\sigma(\theta)-\theta,\sigma\in G$. 根据 M 的定义，$\mathcal{P}(\theta)\in N$. 仿照引理 4, 1) 的第一部分的证明，可知 $\chi_\theta(\sigma)\in\mathbf{F}_p$ 对所有 $\sigma\in G$. 因而 χ_θ 是 G 的一个特征标，这样就定义 M 到 $\hat{G}$ 的一个映射 $\eta:\theta\mapsto\chi_\theta$. 易见 η 是一个同态而且 $\ker(\eta)=F^+$, M 在 η 下的同态象记作 $\hat{H}$. $\hat{H}$ 是 $\hat{G}$ 的一个子群. 为了证明 $M=M_K$, M_K 如引理 4 中所规定的，先必需证明 $\hat{H}=\hat{G}$. 为此又先要证明 $\bigcap\limits_{\chi\in\hat{H}}\ker(\chi)=\{1\}$. 设 $\sigma\in G$ 为任一元素使得对所有 $\theta\in M$ 都有 $\chi_\theta(\sigma)=0$, 于是对所有 $\theta\in M$ 恒有 $\sigma(\theta)-\theta=0$ 即 $\sigma(\theta)=\theta$. 因而 σ 是 K 的一个恒等自同构. 这就证明了

$$\bigcap_{\chi\in\hat{H}}\ker(\chi)=\{1\}.$$

根据引理 2 的推论得 $\hat{H}=\hat{G}$. 由此证明 η 给出了 M 到 $\hat{G}$ 的满同态使得 $M/F^+\cong\hat{G}$. 从而推出，$\theta_1,\cdots,\theta_r$ 和 F^+ 生成 M 当而且仅当 $\chi_{\theta_1},\cdots,\chi_{\theta_r}$ 生成 $\hat{G}$. 由引理 4 推出 $M=M_K$, 即 $\mathcal{P}^{-1}(N)=M_K$. □

习 题

1. (i) 若 F 为一域，且 $\eta:F\to F$ 是一个环同态，则 $\eta=0$ 或 η 是一个单一同态而且 $\eta(1)=1$.

(ii) 域 F 到自身的环自同构全体 $\mathrm{Aut}F$ 对映射的合成运算成一群.

(iii) 设 K/F 为任一域扩张, 则 K 的 F- 自同构全体 $\mathrm{Gal}(K/F)$ 是 $\mathrm{Aut}K$ 的一个子群.

(iv) 设 K/F 为一代数扩张, 则 K 的任一个 F- 自同态都是 F- 自同构.

2. 域 F 的每个非零自同态都保持 F 内素域的元素不动. 设 P 为含于 F 内的素域, 于是 $\mathrm{Aut}F = \mathrm{Gal}(F/P)$.

*3. 证明 $\mathrm{Gal}(\mathbf{R}/\mathbf{Q}) = \{1\}$, 其中 $\mathbf{R}$ 为实数域, $\mathbf{Q}$ 为 $\mathbf{R}$ 中的素域即有理数域.

4. 决定 $\mathrm{Gal}(K/\mathbf{Q})$, 其中 $K = \mathbf{Q}(\sqrt{2}, \sqrt{3})$.

5. 设 $p_1, \cdots, p_r$ 为 r 个不同的有理素数, 决定 $\mathrm{Gal}(K/\mathbf{Q})$, 其中 $K = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \cdots, \sqrt{p_r})$.

6. 设 F 为多项式环 $\mathbf{F}_p[t]$ 的商域, 即 $F = \mathbf{F}_p(t)$. 令 K 为多项式 $f(x) = x^p - t$ 在 F 上的分裂域. 证明 $\mathrm{Gal}(K/F) = \{1\}$.

7. 设 $F = \mathbf{F}_p(t)$ 如习题 6. 令 K 为 $f(x) = x^{2p} + tx^p + t$ 在 F 上的分裂域. 试决定 $\mathrm{Gal}(K/F)$, 并定出 $\mathrm{Gal}(K/F)$ 的不动域和 F 在 K 内的可分闭包.

8. 设 $K = F(t)$ 为单超越扩张. K 的元素 u 可唯一地写成

$$u = \frac{\varphi(t)}{\psi(t)},$$

$\varphi(t), \psi(t) \in F[t]$ 且 $(\varphi(t), \psi(t)) = 1$. 证明:

(i) 若 $u \notin F$, 则 u 在 F 上超越. 此时 K 的中间域 $L = F(u)$ 也是一个单超越扩张.

(ii) 设 $u \notin F$, 令 $m = \max(\deg\varphi(t), \deg\psi(t))$. 则 $m \geq 1$, 而且 t 是 L 上多项式环 $L[x]$ 的 m 次多项式

$$f(x) = \psi(x)u - \varphi(x) = a_0(u)x^m + a_1(u)x^{m-1} + \cdots + a_m(u)$$

的一个根, 其中 $a_i(u)$ 作为 u 的多项式, 次数都不超过 1. 证明 $f(x)$ 在 L 上不可约. [可仿照第四章 §4 艾森斯坦多项式的不可约性的证明, 首先指出 $f(x)$ 没有次数 ≥ 1 且属于 $F(x)$ 的因式, 然后证明 $f(x)$ 在 L 的子环 $F[u]$ 上不可约] 从而 $[K:L] = m$.

(iii) $K = F(u)$ 当而且仅当 u 可表成

$$u = \frac{at+b}{ct+d},$$

其中 $a, b, c, d \in F$ 且 $ad - bc \neq 0$.

9. 设 $K = F(t)$ 为单超越扩张. 证明 $G = \mathrm{Gal}(K/F)$ 与商群 $GL(2, F)/F^*E$ 同构, 其中 $GL(2, F)$ 表示 F 上 2×2 可逆矩阵群, E 为单位矩阵. 并且 G 可由下列元素生成

$$\sigma_a : t \mapsto t + a, \quad \tau_b : t \mapsto bt, \quad \rho : t \mapsto t^{-1}, \quad a, b \in F, b \neq 0.$$

10. 证明: 单超越扩张 $\mathbf{F}_2(t)$ 的自同构群与对称群 S_3 同构, 并且它的不动域等于 $\mathbf{F}_2(u)$,

$$u = \frac{(t^4 - t)^3}{(t^2 - t)^5}.$$

11. 设 $E=\mathbf{F}_p(t)$ 为单超越扩张， $\sigma\in\mathrm{Gal}(E/\mathbf{F}_p)$ 使得 $\sigma(t)=t+1$. 令 $G=\langle\sigma\rangle$, 试决定 G 的不动域.

12. 设 $E=\mathbf{C}(t)$ 为复数域 $\mathbf{C}$ 上单超越扩张. 又设 $\sigma,\tau\in\mathrm{Gal}(E/\mathbf{C})$ 使得

$$\sigma(t)=\omega t,\quad \tau(t)=t^{-1},$$

其中 $\omega=\frac{1}{2}(-1+\sqrt{-3})$. 证明：

$$\sigma^3=1=\tau^2,\quad \tau\sigma=\sigma^{-1}\tau.$$

而且 σ,τ 生成一个 6 阶子群，记作 G. 证明 G 的不动域为子域 $\mathbf{C}(u),u=t^3+t^{-3}$.

13. 设 $K=\mathbf{Q}(\sqrt{2},\sqrt{3}),\theta=(9-5\sqrt{3})(2-\sqrt{2}),E=K(\sqrt{\theta})$. 证明 $E/\mathbf{Q}$ 正规，决定 $\mathrm{Gal}(E/\mathbf{Q})$.

14. 设 $K=\mathbf{Q}(\sqrt{2},\sqrt{3}),\theta=(2-\sqrt{2})(3+\sqrt{3}).E=K(\sqrt{\theta})$. 证明 $E/\mathbf{Q}$ 正规并决定 $\mathrm{Gal}(E/\mathbf{Q})$.

15. 设 $E=F(x_1,\cdots,x_n)$ 为域 F 上 n 个未定元 $x_1,\cdots,x_n$ 的有理分式域，它是多项式环 $R=F[x_1,\cdots,x_n]$ 的商环. 对于 n 元对称群 S_n 的每个置换 π. 如书中所规定的， π 决定了 E 的一个 F- 自同构 σ_π. 证明：

(i) 设 $f(x_1,\cdots,x_n),g(x_1,\cdots,x_n)\in R$ 互素，则 $\sigma_\pi\left(\dfrac{f}{g}\right)=\dfrac{f}{g}$ 对所有的 $\pi\in S_n$ 当而且仅当 $\sigma_\pi(f)=f$ 和 $\sigma_\pi(g)=g$ 对所有的 $\pi\in S_n$.

(ii) 设 A_n 为 n 元交错群. 令 $G=\{\sigma_\pi\,|\,\pi\in S_n\},H=\{\sigma_\pi\,|\,\pi\in A_n\}$, 令 K 表示 G 的不动域. 令

$$\Delta_+=\sum_{\pi\in A_n}x^0_{\pi(1)}x^1_{\pi(2)}\cdots x^{n-1}_{\pi(n)},$$
$$\Delta_-=\sum_{\pi\in S_n\setminus A_n}x^0_{\pi(1)}x^1_{\pi(2)}\cdots x^{n-1}_{\pi(n)},$$
$$\Delta=\prod_{i<j}(x_i-x_j).$$

于是 $\Delta=\Delta_+-\Delta_-$, 而且 $K(\Delta_+)=K(\Delta_-)$ 是 H 的不动域. 特别当 F 的特征 $\neq 2$ 时，$K(\Delta)=K(\Delta_+)$.

16. 试定出下列多项式在有理数域 $\mathbf{Q}$ 上的群：

(i) x^3-2x+3;

(ii) x^3-x-1;

(iii) x^3-3x-1;

(iv) x^4-11x^2+30;

(v) x^4-4x^2+5;

(vi) x^4+2x^2+2x+2;

(vii) x^4-10x^2+4;

(viii) x^4+4x^2+2;

(ix) $x^4-8x+12$;

(x) x^4+px+p, p 为素数.

17. 计算

(i) x^3-x-1 在 $\mathbf{Q}(\sqrt{-23})$ 上的群;

(ii) 设 $K/\mathbf{Q}$ 为二次扩张, x^3-3x-1 在 K 上的群;

(iii) x^4-2 在 $\mathbf{Q}(\sqrt{-1})$ 上的群;

(iv) x^4-4x+5 在 $\mathbf{Q}(\sqrt{5})$ 上的群;

(v) $x^4-8x+12$ 在 $\mathbf{Q}$ 的任意二次扩张上的群.

18. 设域 F 的特征 $\neq 2$. 又设 $x^4+ax^2+b\in F[x]$ 不可约, G 为它的群. 于是

(i) 若 b 是 F 的一个平方数, 则 G 与四元群 $\langle(12)(34),(13)(24)\rangle$ 同构.

(ii) 若 b 不是 F 的平方数而且 $b(a^2-4b)$ 是 F 的一个平方数, 则 G 是一个循环群.

(iii) 若 b 和 $b(a^2-4b)$ 在 F 内都不是平方数, 则 G 与 8 阶的二面体群 D_4 同构.

19. 试决定 x^4-2 在 $\mathbf{Q}$ 上的群以及 x^4-2 在 $\mathbf{Q}$ 上的分裂域的所有子域.

20. 设域 F 的特征 $\neq 2$. 如果 F 包含一个本原的 n 次单位根而且 n 为奇数, 则 F 包含一个本原的 $2n$ 次单位根.

21. 设 F 是 $\mathbf{Q}$ 上的一个有限扩张. 证明 F 只包含有限多个单位根.

22. 用 ζ_n 表示一个本原的 n 次单位根.

(i) 找出 $\mathbf{Q}(\zeta_5)$ 的所有子域;

(ii) 找出 $\mathbf{Q}(\zeta_8)$ 的所有子域;

(iii) 设 $n>2$, 证明 $\mathbf{Q}(\zeta_n+\zeta_n^{-1})$ 是 $\mathbf{Q}(\zeta_n)$ 中的最大实子域. (先指出 $\mathbf{Q}(\zeta_n)$ 有一个 2 阶自同构 $\zeta_n\to\zeta_n^{-1}$, 就是复数域 $\mathbf{C}$ 的复共轭 $a+b\sqrt{-1}\mapsto a-b\sqrt{-1}$ 在 $\mathbf{Q}(\zeta_n)$ 上诱导出的自同构.)

23. 设 p 为一奇素数. 证明:

(i) $\mathbf{Z}_{p^n}=\mathbf{Z}/(p^n)$, $n\geq 1$, 的单位群 $(\mathbf{Z}_{p^n})^*$ 是一个 $(p-1)p^{n-1}$ 阶循环群. (先指出 $1+p$ 在 $(\mathbf{Z}_{p^n})^*$ 中代表一个 p^{n-1} 阶元. 其次, 令 g_1 为模 p 的一个原根, 而且令 $g_1^{p^{n-1}}\equiv g \pmod{p^n}$, $1\leq g<p^n$, 则 g 在 $(\mathbf{Z}_{p^n})^*$ 中代表一个 $p-1$ 阶元.)

(ii) p^n $(n\geq 1)$ 分圆域 $\mathbf{Q}(\zeta_{p^n})$ 是 $\mathbf{Q}$ 上的 $(p-1)p^{n-1}$ 次循环扩张.

24. 证明:

(i) $\mathbf{Z}_{2^n}=\mathbf{Z}/(2^n)$, $n>2$, 的单位群 $(\mathbf{Z}_{2^n})^*$ 是一个 2^{n-2} 阶循环子群 $\langle 5\rangle$,(5 简单表示以 5 为代表 mod 2^n 的陪集) 和一个 2 阶子群 $\langle -1\rangle$ 的直积.

(ii) 2^n, $n>2$, 分圆域 $\mathbf{Q}(\zeta_{2^n})$ 在 $\mathbf{Q}$ 上的伽罗瓦群与直积 $\langle 5\rangle\times\langle -1\rangle$ 同构, 其中 $\langle 5\rangle$ 和 $\langle -1\rangle$ 如 i) 中所定义的.

25. 设 p 为一奇素数, 令 $p^*=(-1)^{\frac{p-1}{2}}p$. 证明: p^n, $n\geq 1$, 分圆域 $\mathbf{Q}(\zeta_{p^n})$ 包含一个唯一的 2 次子域 $\mathbf{Q}(\sqrt{p^*})$.

26. 证明: 2^n, $n\geq 3$, 分圆域 $\mathbf{Q}(\zeta_{2^n})$ 恰好包含三个 2 次子域 $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{-1})$ 和 $\mathbf{Q}(\sqrt{-2})$.

27. 设 E/F 为一个有限伽罗瓦扩张, $G=\mathrm{Gal}(E/F)$. 设 K 为 E/F 的任一中间域, $H=\mathrm{Gal}(E/K)$. 令 $N=\{\sigma\in G\,|\,\sigma(K)=K\}$. 证明:

(i) N 是 H 在 G 中的正规化子;

(ii) $\mathrm{Gal}(K/F)\cong N/H$.

28. 举例说明，存在 $\mathbf{Q}$ 上的一个根式扩张链

$$\mathbf{Q} = F_0 \subset F_1 \subset \cdots \subset F_r = K,$$

但是 $K/\mathbf{Q}$ 有一个中间域 $L/\mathbf{Q}$ 使得 $L/\mathbf{Q}$ 不能写成一个根式扩张链.

29. 在 $\mathbf{Q}$ 上用根式解方程 $x^7 - 1 = 0$.

30. 设 $f(x) \in \mathbf{Q}[x]$ 是一个 n $(n > 4)$ 次不可约多项式而且 $f(x)$ 在 $\mathbf{Q}$ 上的群 $G \cong S_n$. 设 $E/\mathbf{Q}$ 为 $f(x)$ 的分裂域，$\alpha \in E$ 为 $f(x)$ 的一根. 证明：

(i) $\mathrm{Gal}(\mathbf{Q}(\alpha)/\mathbf{Q}) = 1$ 但 $[\mathbf{Q}(\alpha) : \mathbf{Q}] = n$.

(ii) $\mathbf{Q}(\alpha)$ 在 $\mathbf{Q}$ 上的正规闭包 (把它看作 E 的子域) 就是 E.

31. 设 $f(x) = x^3 + ax^2 + bx + c \in \mathbf{Q}[x]$ 为任一三次多项式，D 表示 $f(x)$ 的判别式. 证明：$f(x)$ 有重根或有三个不同的实根或有一对复根 (非实) 和一实根，按照 $D = 0$ 或 $D > 0$ 或 $D < 0$ 而定.

32. p 元域 $\mathbf{F}_p$ 上的变换 $\eta : x \mapsto ax + b, a, b \in \mathbf{F}_p, a \neq 0$, 叫做 $\mathbf{F}_p$ 上的仿射变换. 它也是 $\{0, 1, \cdots, p-1\}$ 的一个置换. $\mathbf{F}_p$ 上仿射变换全体对映射的合成构成一个群，记作 A. 证明：

(i) A 的阶 $= p(p-1)$, A 是一个传递群.

(ii) A 的平移 $\sigma_b : x \mapsto x + b, b = 0, 1, \cdots, p-1$, 构成 A 的一个 p 阶循环子群 P, 每个 $\sigma_b, 1 \le b < p$, 无不动点.

(iii) A 的旋转 $\tau_a : x \mapsto ax, a = 1, \cdots, p-1$, 构成 A 的 $p-1$ 阶循环子群 H_0. 每个 $\tau_a, 1 < a < p$, 只有一个不动点 0.

(iv) $\tau_a \sigma_b \tau_{a^{-1}} = \sigma_{ab}$. P 在 A 内正规，因而 P 是 A 的唯一的 p 阶子群.

(v) 令 $H_b = \sigma_b H_0 \sigma_{-b}$, $b = 0, 1, \cdots, p-1$, 是与 H_0 共轭的子群，每个 $\sigma_b \tau_a \sigma_{-b}$ 只有一个不动点 b, 且

$$\sigma_b \tau_a \sigma_{-b}(x) = ax + b(1-a).$$

(vi) A 是一个可解群，而且 A 的任何正规子群除 $\{1\}$ 外都包含 P.(指出 A 的 $\{1\}$ 以外的正规子群都是传递的.)

33. p 元置换群 A, H_0, P 定义如习题 32. A 看作 p 元对称群 S_p 的子群. 证明：

(i) P 是 S_p 的一个西罗 p- 子群，P 在 S_p 内的中心化子就是 P 自己.

(ii) P 在 S_p 内的正规化子就是 A.

(iii) 设 B 为 S_p 的任一个可解的传递群. 证明 B 的西罗 p- 子群在 B 内是正规的，因而是唯一的，记作 P'. 于是 P' 在 S_p 内的正规化子，记作 N', 包含 B.

(iv) B 与 A 的一个子群共轭.

34. (伽罗瓦) 设域 F 的特征 $= 0$, $f(x) \in F[x]$ 为一素数 p 次不可约多项式，E/F 为它的分裂域. 证明 $f(x)$ 可用根式解的充要条件是 E 可由 $f(x)$ 的任意两根 α, β 生成，即 $E = F(\alpha, \beta)$.(充分性证明. 对 $f(x)$ 的根 $\alpha_1, \cdots, \alpha_p$ 可考虑子群 $G_i = \mathrm{Gal}(E/F(\alpha_i))$. 指出 $G_i \cap G_j = \{1\}, i \neq j$. 由此证明，$G = \mathrm{Gal}(E/F)$ 的西罗 p- 子群是正规的.)

35. 具体写出下列多项式在指定域上的群：

(i) x^5-2 在 $\mathbf{Q}$ 上的群;

(ii) x^5-2 在 $\mathbf{Q}(\sqrt{5})$ 上的群.

36. 设 p 为一素数. 证明: x^p-2 在 $\mathbf{Q}$ 上的群和 $\mathbf{F}_p$ 上仿射群同构, 并具体写出同构.

37. 设 E/F 为一素数 p 次循环扩张, L/F 为任一域扩张. 证明: 复合域 $E\cdot L$ 或者仍然是 L 上的 p 次循环扩张或者 $E\cdot L=L$. 若为前者, $E\cdot L/L$ 有可能还是一个根式扩张.

38. $\mathbf{Q}$ 上有限扩张 $K/\mathbf{Q}$ 在本题中都看作复数域 $\mathbf{C}$ 的子域. 若 K 还包含在实数域 $\mathbf{R}$ 中, 则 K 称为一个实域, 或称为一个实有限扩张. 如果 K/F 是一个实有限扩张同时又是一个根式扩张, 则 K/F 叫做一个实根式扩张. 如果 $\mathbf{Q}$ 上一个多项式 $f(x)$ 的分裂域 $E/\mathbf{Q}$ 包含在一个实根式扩张 $K/\mathbf{Q}$ 中, 则称 $f(x)$ 是可以用实根式解的. 我们在下面将要证明. 在 $\mathbf{Q}$ 上存在这样的不可约多项式 $f(x)$, 它是可以用根式解的, 而且 $f(x)$ 的根都是实根. 但是 $f(x)$ 是不能用实根式解的. 以 x^3-3x+1 为例, 证明:

(i) $f(x)=x^3-3x+1$ 在 $\mathbf{Q}$ 上不可约, 有三实根, 而且 $f(x)$ 在 $\mathbf{Q}$ 上的分裂域 $E/\mathbf{Q}$ 是一个 3 次 (实) 循环扩张.

(ii) 设 $K/\mathbf{Q}$ 为任一实有限扩张. 证明复合域 $E\cdot K$ 或者是 K 上的一个 3 次实循环扩张或者 $EK=K$. 若为前者, EK 决不是 K 上的根式扩张.

(iii) 设 $K/\mathbf{Q}$ 为一个实根式扩张, 则复合域 $E\cdot K$ 恒为 K 上一个 3 次实循环扩张但决非 (实) 根式扩张. 因此 $f(x)=x^3-3x+1$ 不能用实根式解.

39. 证明 $x^5+20x+16$ 在 $\mathbf{Q}$ 上的群为 S_5.

40. 证明 $f(x)=x^6+22x^5-9x^4+12x^3-29x-15$ 在 $\mathbf{Q}$ 上的群为 S_6.

41. 作一个群为 S_4 的有理系数四次多项式.

42. 设 E/F 是一个 p^n(p 为素数、$n\geq 1$) 次循环扩张. 又设 L 是 E/F 的一个中间域使得 $[E:L]=p$. 证明: 若 E 可由元素 α 在 L 上生成, 则 E 也可由元素 α 在 F 上生成.

43. 设域 F 的特征为素数 p. 又设 E/F 为一个 p^n 次 ($n\geq 1$) 循环扩张而且 $\mathrm{Gal}(E/F)=\langle\sigma\rangle$. 证明:

(i) 存在 E 的元素 γ 使得 $T_F^E(\gamma)=1$. 对 γ 又存在 E 的一个元素 β 使得 $\sigma(\beta)-\beta=\gamma^p-\gamma$.

(ii) 设 β 如 i) 作出的, 则 $x^p-x-\beta$ 在 E 上不可约.

(iii) 添加 $x^p-x-\beta$ 的一根 α 到 E 得到的扩域 $E(\alpha)$ 是 F 上的 p^{n+1} 次伽罗瓦扩张. (注意, $E(\alpha)$ 是 F 上的伽罗瓦扩张, 其充要条件是 $x^p-x-\sigma(\beta)$ 的根都在 $E(\alpha)$ 中.)

(iv) $E(\alpha)$ 有一个 F- 自同构 τ 使得

$$\tau(\alpha)=\alpha+\gamma.$$

而且 τ 的阶 $=p^{n+1}$. 因而 $E(\alpha)$ 是 F 上一个 p^{n+1} 次循环扩张.

(v) 若在 F 上存在 p 次循环扩张, 则在 F 上存在任意 p^n 次循环扩张. 反之显然.

44. 设域 F 的特征为素数 p, 则在 F 上存在任意 p^n 次循环扩张的充要条件是 F 的加法子群 $\mathcal{P}(F^+)$ 小于 F^+.

45. (i) 设 F 为 p^n (p 素数) 个元素的有限域, 证明群指数 $(F^+:\mathcal{P}(F^+))=p$.

(ii) 设 F 为特征 $p\ (p>0)$ 的域，$K=F(t), t$ 在 F 上超越. 证明 $(K^+ : \mathcal{P}(K^+))>1$.

46. (i) 证明：当素数 $p>7$ 时，x^7-1 在素域 $\mathbf{F}_p$ 上可以用根式解，并具体求出它的解.

(ii) 证明 x^7-1 在素域 $\mathbf{F}_3$ 上不能用根式解. 但可以应用本章定理 27 求解. 并具体写出它的解.

第九章　多重线性代数初步

近年来，多重线性代数的概念已经成为数学许多分支常用的工具．在这一章我们将对多重线性代数作一初步的介绍．

作为线性变换与线性函数的推广，我们首先引进多重线性变换与多重线性函数的概念，然后给出线性空间的张量积与张量代数，在张量代数的基础上利用交错化算子定义外乘积与外代数．

§1　对偶空间

我们已经介绍过线性空间上线性函数的概念，现在着重来考察一下线性函数组成的空间，即所谓**对偶空间**．

在这一章我们总是假定 F 是一个任意域，而讨论的线性空间都是指域 F 上的线性空间．

为了统一线性变换与线性函数，我们首先把以前的线性变换的定义稍作推广．

定义 1　设 V 与 W 是域 F 上的两个线性空间，$\boldsymbol{A}$ 是 V 到 W 的一个映射．如果 $\boldsymbol{A}$ 适合：

1) $\boldsymbol{A}(\alpha+\beta)=\boldsymbol{A}(\alpha)+\boldsymbol{A}(\beta)$,

2) $\boldsymbol{A}(k\alpha)=k\boldsymbol{A}(\alpha)$,

对所有的 $\alpha,\beta\in V$, $k\in F$，那么 $\boldsymbol{A}$ 就称为**由 V 到 W 的一个线性变换**．

显然，在 $V=W$ 的情形，这就是过去所说的线性变换．我们知道，F 可以看作域 F 上的一个一维线性空间，因此，所谓线性空间 V 的线性函数就是由 V 到 F 的线性变换．

与线性空间到自身的线性变换一样，我们有

定理 1　设 V, W 是域 F 上线性空间，V 的维数为 n, $\varepsilon_1,\cdots,\varepsilon_n$ 是 V 的一组基．对于 W 中任意 n 个元素 $\beta_1,\cdots,\beta_n$．存在唯一的线性变换 $\boldsymbol{A}:V\to W$ 使

$$\boldsymbol{A}(\varepsilon_i)=\beta_i,\ i=1,\cdots,n.$$

证明留给读者．□

当 V 与 W 都是有限维线性空间时，我们也可以谈线性变换 $\boldsymbol{A}:V\to W$ 的矩阵，不过要在线性空间 V 与 W 中都各自取一组基．读者不难写出线性变换与矩阵之间对应的细节，这里就不多谈了．

在线性空间 V 的线性函数之间我们可以定义运算，设 f,g 是 V 的任意两个线性函数，k 是域 F 中任意元素. 我们定义

$$(f+g)(\alpha)=f(\alpha)+g(\alpha),$$
$$(kf)(\alpha)=kf(\alpha).$$

容易验证，这样定义的 $f+g$ 与 kf 仍然是线性函数，而且线性空间 V 的全体线性函数在这两个运算下也构成域 F 上的线性空间.

定义 2 设 V 是域 F 上一线性空间. V 的全体线性函数在上面定义的两个运算下所成的线性空间称为 V 的 **对偶空间**, 记为 V^*.

下面我们主要来考察有限维线性空间的对偶空间. 对于有限维线性空间的线性函数，我们有以下的基本事实.

推论 设 V 是域 F 上一 n 维线性空间，$\varepsilon_1,\cdots,\varepsilon_n$ 是 V 的一组基. 对 F 中任意给定的 n 个元素 $b_1,\cdots,b_n$, 存在 V 的唯一的一个线性函数 f 使

$$f(\varepsilon_i)=b_i,\quad i=1,\cdots,n.$$

证明留给读者. □

由此我们可以立即证明

定理 2 设 V 是域 F 上一 n 维线性空间，$\varepsilon_1,\cdots,\varepsilon_n$ 是 V 的一组基. V 的对偶空间 V^* 也是 n 维的，而且 V^* 有一组基 $f_1,\cdots,f_n$ 适合条件

$$f_i(\varepsilon_j)=\delta_{ij}\quad i,j=1,\cdots,n.$$

证明 由定理 1 的推论，在 V^* 中有 n 个线性函数 $f_1,\cdots,f_n$ 使

$$f_i(\varepsilon_j)=\delta_{ij},\quad i,j=1,\cdots,n.$$

我们来证明，$f_1,\cdots,f_n$ 线性无关且构成 V^* 的一组基.

假设线性组合

$$k_1f_1+\cdots+k_nf_n=0.$$

考察两边在基向量 ε_j 上的函数值，即得

$$\begin{aligned}&(k_1f_1+\cdots+k_nf_n)(\varepsilon_j)\\&\quad=k_1f_1(\varepsilon_j)+\cdots+k_nf_n(\varepsilon_j)\\&\quad=k_j=0.\end{aligned}$$

取 $j=1,\cdots,n$, 这就证明了 $f_1,\cdots,f_n$ 线性无关. 对于任意的 $f\in V^*$, 令

$$f(\varepsilon_j)=b_i,\ \ j=1,\cdots,n.$$

显然

$$(b_1f_1+\cdots+b_nf_n)(\varepsilon_j)=b_j,\ \ j=1,\cdots,n.$$

由定理 1 的唯一性即得

$$f=b_1f_1+\cdots+b_nf_n.$$

这就是说, V^* 中任一元素都可以表成 $f_1,\cdots,f_n$ 的线性组合, 因而 $f_1,\cdots,f_n$ 是 V^* 的一组基, V^* 是 n 维的. □

定理 2 中所作的 V^* 的基 $f_1,\cdots,f_n$ 称为 V 的基 $\varepsilon_1,\cdots,\varepsilon_n$ 的 **对偶基**.

推论 设 V 是域 F 上一 n 维线性空间, α 是 V 中一个向量. 如果对于所有的 $f\in V^*$ 都有 $f(\alpha)=0$, 那么 $\alpha=0$.

证明 在 V 中取一组基 $\varepsilon_1,\cdots,\varepsilon_n$, 令 $f_1,\cdots,f_n$ 是它的对偶基. 设

$$\alpha=a_1\varepsilon_1+\cdots+a_n\varepsilon_n,$$

由条件, $f_i(\alpha)=a_i=0,\ i=1,\cdots,n$. 于是

$$\alpha=0.\ \ □$$

线性空间 V 的对偶空间 V^* 也是线性空间, 当然也可以考虑它的对偶空间 V^{**}. 由定理 2, 如果 V 是 n 维的, 那么 V^*, 从而 V^{**} 都是 n 维的. 下面来建立 V 与 V^{**} 的一个重要联系. 设 $\alpha\in V$ 是一固定的向量, 对于所有的 $f\in V^*$,

$$f\mapsto f(\alpha)$$

定义了 V^* 到 F 的一个映射. 容易验证, 这是 V^* 的一个线性函数. 我们记这个线性函数为 α^*, 上面的定义可以写成

$$\alpha^*(f)=f(\alpha). \tag{1}$$

按这个方式我们建立了 V 到 V^{**} 的一个映射. 我们来证明它是 V 到 V^{**} 的一个线性变换.

任取 $\alpha,\beta\in V$, $k\in F$, 我们有

$$\begin{aligned}(\alpha+\beta)^*(f)&=f(\alpha+\beta)\\&=f(\alpha)+f(\beta)\\&=\alpha^*(f)+\beta^*(f)\\&=(\alpha^*+\beta^*)(f),\\(k\alpha)^*(f)&=f(k\alpha)=kf(\alpha)=k(\alpha^*(f))\\&=(k\alpha^*)(f).\end{aligned}$$

换句话说,

$$(\alpha+\beta)^*=\alpha^*+\beta^*,$$
$$(k\alpha)^*=k\alpha^*.$$

这就证明了映射 $\alpha\mapsto\alpha^*$ 是 V 到 V^{**} 的一个线性变换.

定理 2 的推论表明, 如果 $\alpha\neq 0$, 那么 $\alpha^*\neq 0$, 即把非零元素映到非零元素. 因之, 这个线性变换是单射的.

在 V 中取一组基 $\varepsilon_1,\cdots,\varepsilon_n$, 令 $f_1,\cdots,f_n\in V^*$ 是它的对偶基. 由 (1) 可知

$$\varepsilon_i^*(f_j)=f_j(\varepsilon_i)=\delta_{ij},\quad i,j=1,\cdots,n.$$

这就是说, $\varepsilon_1^*,\cdots,\varepsilon_n^*$ 恰好是 $f_1,\cdots,f_n$ 的对偶基. 既然 $\varepsilon_1^*,\cdots,\varepsilon_n^*$ 是 V^{**} 的一组基, 所以这个线性变换是满的.

综合以上讨论, 由 (1) 所定义的映射

$$\alpha\mapsto\alpha^*$$

是线性空间 V 到线性空间 V^{**} 的一个同构映射. 在这个同构映射下, 如果我们把 α 与 α^* 等同起来, 那么就可以把 V 也看作是 V^* 的对偶空间, 或者说, V^* 的元素是 V 的线性函数, 而 V 的元素按 (1) 也可以看作是 V^* 的线性函数.

应该指出, 对于有限维线性空间 V, 线性空间 V,V^* 与 V^{**} 有相同的维数, 按线性空间的一般理论, 它们当然是同构的. 上面按 (1) 定义的同构映射的意义不在于说明 V 与 V^{**} 是同构, 而在于给出了一个特定的同构映射, 在这个映射下, V 的元素与 V^{**} 的元素之间建立了对应. 以后将会看到, 这个映射具有很好的性质, 这里就不细说了.

§2 多重线性函数

作为线性变换与线性函数的推广, 我们来定义多重线性变换与多重线性函数.

定义 3 设 $V_1,\cdots,V_r$ 与 W 是域 F 上的线性空间, 映射

$$\boldsymbol{A}:V_1\times\cdots\times V_r\to W$$

称为**多重线性变换**, 如果对于所有的 $\alpha_i,\beta_i\in V_i$, $i=1,\cdots,r$, 所有的 $k\in F$, 它适合

1) $\boldsymbol{A}(\alpha_1,\cdots,\alpha_i+\beta_i,\cdots,\alpha_r)=\boldsymbol{A}(\alpha_1,\cdots,\alpha_i,\cdots,\alpha_r)+\boldsymbol{A}(\alpha_1,\cdots,\beta_i,\cdots,\alpha_r)$;

2) $\boldsymbol{A}(\alpha_1,\cdots,k\alpha_i,\cdots,\alpha_r)=k\boldsymbol{A}(\alpha_1,\cdots,\alpha_i,\cdots,\alpha_r)$, $i=1,\cdots,r$.

由定义可以看出，所谓多重线性变换就是对每一个变元都是线性的，或者说，如果固定其中的 $r-1$ 个变元，那么对于剩下的那个变元，它是一个线性变换．当 $r=1$ 时，这就是通常的线性变换，当 $r=2$ 时，它通常称为双线性变换．多重线性变换有不少性质与线性变换相仿，这里不多说了．

定义 4 设 $V_1,\cdots,V_r$ 是域 F 上的线性空间．由 $V_1,\cdots,V_r$ 到 F 的多重线性变换称为定义在 $V_1,\cdots,V_r$ 上的 **多重线性函数**.

显然，这是我们已经知道的线性函数与双线性函数的推广．和线性函数一样，对于多重线性函数我们也可以定义加法与数量乘法．设 f,g 是定义在线性空间 $V_1,\cdots,V_r$ 上线性函数， $k\in F$. 对于 $\alpha_i\in V_i$, $i=1,\cdots,r$, 我们定义

$$(f+g)(\alpha_1,\cdots,\alpha_r)=f(\alpha_1,\cdots,\alpha_r)+g(\alpha_1,\cdots,\alpha_r),$$
$$(kf)(\alpha_1,\cdots,\alpha_r)=kf(\alpha_1,\cdots,\alpha_r).$$

我们用 $P(V_1,\cdots,V_r)$ 代表定义在线性空间 $V_1,\cdots,V_r$ 上的全体多重线性函数．容易验证， $P(V_1,\cdots,V_r)$ 在上面定义的两个运算下成为域 F 上一个线性空间．

与线性函数的情况相仿，我们有

定理 3 设 $V_1,\cdots,V_r$ 是域 F 上的线性空间， V_i 的维数为 n_i, $\varepsilon_{i1},\cdots,\varepsilon_{in_i}$ 是 V_i 的一组基， $i=1,\cdots,r$. 对域 F 中任意一组元素 $b_{j_1\cdots j_r}$, $j_i=1,\cdots,n_i$ $(i=1,\cdots,r)$, 存在唯一的一个多重线性函数 f 使

$$f(\varepsilon_{1j_1},\cdots,\varepsilon_{rj_r})=b_{j_1\cdots j_r},\quad j_i=1,\cdots,n_i\ (i=1,\cdots,r).$$

证明留给读者． □

对于任意给定的一组脚标 $k_1,\cdots,k_r$, 取

$$b_{j_1\cdots j_r}=\delta_{j_1k_1}\cdots\delta_{j_rk_r},\ j_i=1,\cdots,n_i\ (i=1,\cdots,r).$$

由定理 3, 我们有多重线性函数 $f_{k_1\cdots k_r}$ 使

$$f_{k_1\cdots k_r}(\varepsilon_{1j_1},\cdots,\varepsilon_{rj_r})=\delta_{j_1k_1}\cdots\delta_{j_rk_r},\quad j_i=1,\cdots,n_i\ (i=1,\cdots,r).$$

这样得到的函数 $f_{k_1\cdots k_r}$ 就是

$$f_{k_1\cdots k_r}(\varepsilon_{1k_1},\cdots,\varepsilon_{rk_r})=1,$$

而在基向量的其它组合处取值全为零．

定理 4 符号同定理 3. 上面定义的函数 $f_{k_1,\cdots,k_r}$, $k_i=1,\cdots,n_i$ $(i=1,\cdots,r)$ 线性无关，且构成 $P(V_1,\cdots,V_r)$ 的一组基． $P(V_1,\cdots,V_r)$ 的维数为 $n_1\cdots n_r$.

证明留给读者. □

元素取自域 F 的 n 元数组

$$\alpha=\begin{pmatrix}a_1\\ \vdots\\ a_n\end{pmatrix}$$

的全体在有关运算下，构成域 F 上一个 n 维线性空间 F^n. $n\times n$ 矩阵的行列式

$$\begin{vmatrix}a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{vmatrix}$$

可以看成是 n 个列向量

$$\alpha_i=\begin{pmatrix}a_{1i}\\ a_{2i}\\ \vdots\\ a_{ni}\end{pmatrix},\quad i=1,\cdots,n$$

的函数. 由行列式的性质立即可以看成，行列式是定义在 $F^n,\cdots,F^n$(n 个) 上的一个多重线性函数.

我们现在来建立多重线性函数之间的一种运算. 为了避免过于复杂的脚标，同时也考虑到下一节的直接应用，我们把讨论限制在简单的情形，在弄清楚这种简单的情形之后，推广到一般的情形对于读者将不是困难的事.

设 V 与 W 是域 F 上的线性空间，维数分别是 n 与 m, 而 V^* 与 W^* 分别是它们的对偶空间. 对于 $f\in V^*, g\in W^*$, 我们定义

$$f\otimes g(\alpha,\beta)=f(\alpha)g(\beta),\quad \alpha\in V,\beta\in W.$$

容易验证，对于 $\alpha_1,\alpha_2\in V, k\in F$, 有

$$\begin{aligned}f\otimes g(\alpha_1+\alpha_2,\beta)&=f(\alpha_1+\alpha_2)g(\beta)\\ &=f(\alpha_1)g(\beta)+f(\alpha_2)g(\beta)\\ &=f\otimes g(\alpha_1,\beta)+f\otimes g(\alpha_2,\beta),\\ f\otimes g(k\alpha,\beta)&=f(k\alpha)g(\beta)=kf(\alpha)g(\beta)\\ &=k(f\otimes g)(\alpha,\beta).\end{aligned}$$

因之，$f\otimes g$ 对于 V 是线性的. 同时可以证明，它对于 W 也是线性的. 这就是说，$f\otimes g$ 是定义在 V,W 上的一个双线性函数，即

$$f\otimes g\in P(V,W).$$

这样，我们定义了一个映射

$$\sigma: V^*\times W^*\mapsto P(V,W).$$

显然，映射 σ 对于 V^* 与 W^* 是双线性的. 换句话说，σ 是由 V^* 与 W^* 到 $P(V,W)$ 的一个双线性变换.

在 V 与 W 中分别取基 $\varepsilon_1,\cdots,\varepsilon_n$ 与 $\eta_1,\cdots,\eta_m$，令 $f_1,\cdots,f_n$ 与 $g_1,\cdots,g_m$ 分别是它们的对偶基. 由定理 4 可知，

$$f_i\otimes g_j,\quad i=1,\cdots,n,\quad j=1,\cdots,m$$

构成 $P(V,W)$ 的一组基. 由此可知，虽然 $\sigma(V^*\times W^*)$ 在 $P(V,W)$ 内不构成一个子空间，（为什么？）但是 $\sigma(V^*\times W^*)$ 包含了 $P(V,W)$ 的一组基，因而，$\sigma(V^*\times W^*)$ 生成整个空间 $P(V,W)$.

根据以上讨论，我们可以证明

定理 5 *符号同上. 如果 $\mu_1,\cdots,\mu_n$ 与 $\nu_1,\cdots,\nu_m$ 分别是 V^* 与 W^* 的基，那么 $\mu_i\otimes\nu_j,\ i=1,\cdots,n,\ j=1,\cdots,m$ 是 $P(V,W)$ 的一组基.*

证明 对于任意的 $f\in V^*,g\in W^*$，设

$$f=\sum_{i=1}^n a_i\mu_i,\quad g=\sum_{j=1}^m b_j\nu_j,$$

由双线性，有

$$f\otimes g=\sum_{i=1}^n\sum_{j=1}^m a_ib_j\mu_i\otimes\nu_j.$$

这就是说，$\sigma(V^*\times W^*)$ 中每个元素都可以表成 $\mu_i\otimes\nu_j,\ i=1,\cdots,n,\ j=1,\cdots,m$. 的线性组合，从而 $P(V,W)$ 中每个元素都可以由它们线性表出. 因为 $P(V,W)$ 的维数是 nm，所以它们必线性无关，因而是 $P(V,W)$ 的一组基，这就证明了定理. □

§3 线性空间的张量积

在以上准备工作的基础上，我们现在来定义线性空间的张量积，它是多重线性代数的一个基本概念.

定义 5 设 V_1, V_2 与 W 是域 F 上的线性空间，$\sigma: V_1 \times V_2 \to W$ 是由 V_1, V_2 到 W 的一个双线性变换. 如果对于域 F 上任意的线性空间 U, 任意一个双线性变换 $\varphi: V_1 \times V_2 \to U$, 都存在唯一的线性变换 $\psi: W \to U$ 使

$$\varphi = \psi\sigma,$$

那么 W 就称为 V_1 与 V_2 的一个 **张量积**.

这个定义看起来比较抽象, 不容易把握住张量积究竟是什么, 但是它的确抓住了张量积的特征性质, 以后用起来很方便. 直接从这个定义一下子看不出，对于线性空间这样的张量积是否存在，因之证明它的存在性与唯一性是首先要解决的问题，而在解决这些问题的过程中对于张量积就可以有比较具体的了解.

定理 6 *设 V_1, V_2 是域 F 上有限维线性空间. 线性空间 V_1, V_2 的张量积存在，而且在同构的意义下是唯一的.*

证明 令 V_1^* 与 V_2^* 分别是 V_1 与 V_2 的对偶空间. 我们知道，V_1 与 V_2 可以分别等同于 V_1^{**} 与 V_2^{**}. 按 §2 的讨论, 我们有一双线性变换 $\sigma: V_1 \times V_2 \to P(V_1^*, V_2^*)$, 即

$$\sigma(\alpha, \beta) = \alpha \otimes \beta, \quad \alpha \in V_1, \beta \in V_2.$$

设 $\varepsilon_1, \cdots, \varepsilon_{n_1}$ 与 $\eta_1, \cdots, \eta_{n_2}$ 分别为 V_1 与 V_2 的基，其中 n_1 为 V_1 的维数，n_2 为 V_2 的维数. 由定理 5,$\sigma(\varepsilon_i, \eta_j) = \varepsilon_i \otimes \eta_j$, $i = 1, \cdots, n_1, j = 1, \cdots, n_2$, 是 $P(V_1^*, V_2^*)$ 的一组基.

我们现在来证明，$P(V_1^*, V_2^*)$ 就是 V_1, V_2 的一个张量积. 设 U 是域 F 上任意一个线性空间，$\varphi: V_1 \times V_2 \mapsto U$ 是一个双线性变换. 令

$$\varphi(\varepsilon_i, \eta_j) = \gamma_{ij}, \quad i = 1, \cdots, n_1, \ j = 1, \cdots, n_2,$$

由定理 5 和定理 1, 存在线性变换 $\psi: P(V_1^*, V_2^*) \to U$ 使

$$\psi(\varepsilon_i \otimes \eta_j) = \gamma_{ij}, \quad i = 1, \cdots, n_1, \ j = 1, \cdots, n_2,$$

显然，我们有

$$\psi\sigma(\varepsilon_i, \eta_j) = \varphi(\varepsilon_i, \eta_j), \quad i = 1, \cdots, n_1, \ j = 1, \cdots, n_2,$$

由双线性即得 $\psi\sigma = \varphi$.

如果再有一个线性变换 $\psi_1: P(V_1^*, V_2^*) \to U$ 也适合 $\psi_1\sigma = \varphi$, 那么对于任意的 i, j 有

$$\psi\sigma(\varepsilon_i, \eta_j) = \varphi(\varepsilon_i, \eta_j) = \psi_1\sigma(\varepsilon_i, \eta_j),$$

这就是说， ψ 与 ψ_1 在基向量 $\sigma(\varepsilon_i,\eta_j)$, $i=1,\cdots,n_1,j=1,\cdots,n_2$, 上的象相同. 于是由定理 1 的唯一性即得 $\psi=\psi_1$. 这就说明了，适合条件 $\psi\sigma=\varphi$ 的线性变换 ψ 是唯一的.

以上讨论说明，双线性变换

$$\sigma: V_1\times V_2\to P(V_1^*,V_2^*)$$

满足张量积的定义，因而 $P(V_1^*,V_2^*)$ 就是 V_1,V_2 的一个张量积.

下面再来证明， V_1,V_2 的张量积在同构的意义下是唯一的.

设有双线性变换 σ,σ_1 与线性空间 W,W_1 使

$$\sigma: V_1\times V_2\to W,$$
$$\sigma_1: V_1\times V_2\to W_1$$

都是张量积. 由 W 是张量积，我们有线性变换 $\psi: W\to W_1$, 使

$$\psi\sigma=\sigma_1,$$

再由 W_1 是张量积，我们有线性变换 $\psi_1: W_1\to W$ 使

$$\psi_1\sigma_1=\sigma.$$

令 1_W 与 $1_{W'}$ 分别表示线性空间 W 与 W' 的恒等变换. 根据张量积的定义，对于张量积 W, 另一个双线性变换仍取 $\sigma: V_1\times V_2\to W$, 显然有 $1_W: W\to W$ 使

$$1_W\sigma=\sigma.$$

但是还有线性变换 $\psi_1\psi: W\to W$ 使

$$\psi_1\psi\sigma=\sigma.$$

由定义中要求的唯一性，我们有

$$\psi_1\psi=1_W.$$

同理，有

$$\psi\psi_1=1_{W'}.$$

由此可知， $\psi: W\to W_1$ 是一同构映射，这就证明了，任意两个张量积必同构.

□

逻辑上严格地说，谈到线性空间的张量积时，应同时考虑与之联系的双线性变换

$$\sigma: V_1 \times V_2 \to W.$$

这一点从定理 6 的证明可以看出. 不过为了简单起见，我们总是说“W 是 V_1, V_2 的张量积”，而不明确指出双线性变换.

既然张量积在同构的意义下是唯一的，我们用 $V_1 \otimes V_2$ 表示 V_1, V_2 的张量积，对于

$$\alpha \in V_1, \beta \in V_2,$$

用 $\alpha \otimes \beta$ 表示 $\sigma(\alpha, \beta)$.

根据定义 5 与定理 6，关于张量积，我们有如下的基本性质：

1. $(\alpha_1 + \alpha_2) \otimes \beta = \alpha_1 \otimes \beta + \alpha_2 \otimes \beta$,
   $\alpha \otimes (\beta_1 + \beta_2) = \alpha \otimes \beta_1 + \alpha \otimes \beta_2$.

$$\alpha, \alpha_1, \alpha_2 \in V_1, \beta, \beta_1, \beta_2 \in V_2.$$

2. $(k\alpha) \otimes \beta = \alpha \otimes (k\beta) = k(\alpha \otimes \beta)$. $k \in F, \alpha \in V_1, \beta \in V_2$.

3. 如果 $\varepsilon_1, \cdots, \varepsilon_{n_1}$ 是 V_1 的一组基，$\eta_1, \cdots, \eta_{n_2}$ 是 V_2 的一组基，那么 $\varepsilon_i \otimes \eta_j$, $i = 1, \cdots, n_1, j = 1, \cdots, n_2$, 是 $V_1 \otimes V_2$ 的一组基，因而 $V_1 \otimes V_2$ 的维数为 $n_1 n_2$.

4. $V_1 \otimes V_2$ 中元素都可以表示成

$$\sum_{i=1}^{r} \alpha_i \otimes \beta_j$$

的形式，其中 $\alpha_i \in V_1, \beta_i \in V_2$, $i = 1, \cdots, r$.

定理 7 设 V_1, V_2, V_3 是域 F 上有限维线性空间. 我们有同构映射

$$\psi_1: (V_1 \otimes V_2) \otimes V_3 \to V_1 \otimes (V_2 \otimes V_3)$$

使

$$\psi_1((\alpha \otimes \beta) \otimes \gamma) = \alpha \otimes (\beta \otimes \gamma);$$

有同构映射

$$\psi_2: V_1 \otimes V_2 \to V_2 \otimes V_1$$
$$\psi_2(\alpha \otimes \beta) = \beta \otimes \alpha,$$

其中 $\alpha \in V_1, \beta \in V_2, \gamma \in V_3$.

证明 在 V_1, V_2, V_3 中分别取基 $\varepsilon_1, \cdots, \varepsilon_{n_1}, \eta_1, \cdots, \eta_{n_2}, \xi_1, \cdots, \xi_{n_3}$. 我们知道

$$(\varepsilon_i \otimes \eta_j) \otimes \xi_k \text{ 与 } \varepsilon_i \otimes (\eta_j \otimes \xi_k) \quad i = 1, \cdots, n_1, j = 1, \cdots, n_2, k = 1, \cdots, n_3,$$

分别是 $(V_1\otimes V_2)\otimes V_3$ 与 $V_1\otimes(V_2\otimes V_3)$ 的基. 定义

$$\psi_1:(V_1\otimes V_2)\otimes V_3\to V_1\otimes(V_2\otimes V_3)$$

为

$$\psi_1((\varepsilon_i\otimes\eta_j)\otimes\xi_k)=\varepsilon_i\otimes(\eta_j\otimes\xi_k),\quad i=1,\cdots,n_1, j=1,\cdots,n_2, k=1,\cdots,n_3.$$

显然, ψ_1 即为所要的同构映射. ψ_2 的定义方法类似, 留给读者. □

定理 7 给出了张量积的结合律, 因之在考虑多个线性空间的张量积时, 可以不用括弧. 设 $V_1,\cdots,V_m$ 是 m 个线性空间, 我们可以作它们的张量积:

$$V_1\otimes V_2\otimes\cdots\otimes V_m,$$

也可以考虑形式为

$$\alpha_1\otimes\cdots\otimes\alpha_m,\quad \alpha_i\in V_i,\ i=1,\cdots,m$$

的元素.

在定义了线性空间的张量积之后, 我们再来定义线性变换的张量积.

定理 8 设 V,W 是域 F 上的线性空间, $\boldsymbol{A}:V\to V,\boldsymbol{B}:W\to W$ 是两个线性变换. 于是存在唯一的线性变换 $\boldsymbol{C}:V\otimes W\to V\otimes W$ 使

$$\boldsymbol{C}(\alpha\otimes\beta)=\boldsymbol{A}\alpha\otimes\boldsymbol{B}\beta,\quad \alpha\in V,\beta\in W.$$

证明 定义映射 $\varphi:V\times W\to V\otimes W$ 为

$$\varphi(\alpha,\beta)=\boldsymbol{A}\alpha\otimes\boldsymbol{B}\beta.$$

容易验证, φ 是一双线性变换. 由张量积的定义, 存在唯一的线性变换

$$\boldsymbol{C}:V\otimes W\to V\otimes W$$

使

$$\boldsymbol{C}(\alpha\otimes\beta)=\varphi(\alpha,\beta)=\boldsymbol{A}\alpha\otimes\boldsymbol{B}\beta.\quad □$$

我们称定理 8 中所说的线性变换 C 为线性变换 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ **的张量积**, 记为

$$\boldsymbol{A}\otimes\boldsymbol{B}.$$

读者不难证明线性变换的张量积的一些基本性质:

1. $(\boldsymbol{A}+\boldsymbol{C})\otimes\boldsymbol{B}=\boldsymbol{A}\otimes\boldsymbol{B}+\boldsymbol{C}\otimes\boldsymbol{B}$,
   $\boldsymbol{A}\otimes(\boldsymbol{B}+\boldsymbol{D})=\boldsymbol{A}\otimes\boldsymbol{B}+\boldsymbol{A}\otimes\boldsymbol{D}$.
2. $(\boldsymbol{A}\otimes\boldsymbol{B})(\boldsymbol{C}\otimes\boldsymbol{D})=\boldsymbol{AC}\otimes\boldsymbol{BD}$.
3. $\boldsymbol{E}\otimes\boldsymbol{E}=\boldsymbol{E}$.
4. 如 $\boldsymbol{A},\boldsymbol{B}$ 可逆，则 $\boldsymbol{A}\otimes\boldsymbol{B}$ 也可逆，

$$(\boldsymbol{A}\otimes\boldsymbol{B})^{-1}=\boldsymbol{A}^{-1}\otimes\boldsymbol{B}^{-1}.$$

这里 $\boldsymbol{A},\boldsymbol{C}:V\to V,\boldsymbol{B},\boldsymbol{D}:W\to W$, 而 $\boldsymbol{E}$ 表示单位变换.

下面来看一下，在适当的基下， $\boldsymbol{A}\otimes\boldsymbol{B}$ 的矩阵与 $\boldsymbol{A},\boldsymbol{B}$ 的矩阵的关系.

设 $A=(a_{ij})$ 为一 $n\times n$ 矩阵， $B=(b_{ij})$ 为一 $m\times m$ 矩阵，我们定义

$$A\otimes B=(a_{ij}B),$$

它是一个 $nm\times nm$ 矩阵，称为 A 与 B **的张量积**.

设 $\varepsilon_1,\cdots,\varepsilon_n$ 是 V 的一组基， $\eta_1,\cdots,\eta_m$ 是 W 的一组基，而矩阵 $A=(a_{ij}),B=(b_{ij})$ 分别是线性变换 $\boldsymbol{A},\boldsymbol{B}$ 在这两组基下的矩阵. 我们知道，

$$\varepsilon_1\otimes\eta_1,\cdots,\varepsilon_1\otimes\eta_m,\varepsilon_2\otimes\eta_1,\cdots,\varepsilon_2\otimes\eta_m,\cdots,\varepsilon_n\otimes\eta_1,\cdots,\varepsilon_n\otimes\eta_m$$

是 $V\otimes W$ 的一组基. 读者容易验证，线性变换 $\boldsymbol{A}\otimes\boldsymbol{B}$ 在这组基下的矩阵就是

$$A\otimes B.$$

由线性变换张量积的性质立即可以推出矩阵的张量积的一些基本性质.

最后，我们来看两个例子.

设 V 是域 F 上一个线性空间. 把 F 看作 F 上的一维线性空间，我们可以作张量积

$$F\otimes V.$$

$F\otimes V$ 中的元素为

$$\sum_{i=1}^{r}k_i\otimes\alpha_i=\sum_{i=1}^{r}1\otimes k_i\alpha_i=1\otimes\sum_{i=1}^{r}k_i\alpha_i,$$

这就是说， $F\otimes V$ 的元素全可以表为 $1\otimes\alpha,\alpha\in V$ 的形式.

容易看出，映射 $\varphi:F\times V\to V$,

$$\varphi(k,\alpha)=k\alpha,\quad k\in F,\alpha\in V$$

是双线性的，因而唯一地决定一线性变换

$$\boldsymbol{A}: F \otimes V \to V$$

使

$$\boldsymbol{A}(k \otimes \alpha) = k\alpha.$$

由 $\boldsymbol{A}(1 \otimes \alpha) = \alpha$ 可知 $\boldsymbol{A}$ 是映上的，而 $F \otimes V$ 与 V 有相同的维数，所以，$\boldsymbol{A}$ 是一同构映射. 以后我们常常按这个同构映射把 $F \otimes V$ 与 V 等同起来.

设 V 是实数域 $\mathbf{R}$ 上的一 n 维线性空间. 复数域 $\mathbf{C}$ 可以看作 $\mathbf{R}$ 上的一个二维空间，作

$$\mathbf{C} \otimes V,$$

它是实数域 $\mathbf{R}$ 上的 $2n$ 维线性空间，对于 $z_0 \in \mathbf{C}$, 映射 $z \mapsto z_0 z, z \in \mathbf{C}$, 显然是 $\mathbf{C}$ 的一个线性变换 (把 $\mathbf{C}$ 看作 $\mathbf{R}$ 上的线性空间). 由定理 7, 它决定了 $\mathbf{C} \otimes V$ 到 $\mathbf{C} \otimes V$ 的一个映射

$$z \otimes \alpha \mapsto z_0 z \otimes \alpha.$$

我们定义

$$z_0(z \otimes \alpha) = z_0 z \otimes \alpha.$$

容易验证，在这个运算下，$\mathbf{C} \otimes V$ 构成复数域 $\mathbf{C}$ 上的一个线性空间. 如果 $\varepsilon_1, \cdots, \varepsilon_n$ 是 V 的一组基，那么显然 $1 \otimes \varepsilon_1, \cdots, 1 \otimes \varepsilon_n$ 是 $\mathbf{C} \otimes V$ 作为 $\mathbf{C}$ 上的线性空间的一组基.

$\mathbf{C} \otimes V$ 作为复数域上的线性空间通常称为实数域 $\mathbf{R}$ 上线性空间 V 的 **复化**，或者说，把 V 扩充成一个复数域上的线性空间.

§4　线性空间的直和

定义 6　设 $V_1, \cdots, V_s$ 是域 F 上的线性空间. 考虑所有的 s 元元素组

$$(\alpha_1, \cdots, \alpha_s),\ \alpha_i \in V_i,\ \ i = 1, \cdots, s$$

的集合，定义

$$(\alpha_1, \cdots, \alpha_s) + (\beta_1, \cdots, \beta_s) = (\alpha_1 + \beta_1, \cdots, \alpha_s + \beta_s),$$
$$k(\alpha_1, \cdots, \alpha_s) = (k\alpha_1, \cdots, k\alpha_s),$$

其中 $k \in F, \alpha_i, \beta_i \in V_i$, $i = 1, \cdots, s$. 显然，它构成一线性空间. 这样得到的线性空间称为线性空间 $V_1, \cdots, V_s$ 的 **直和**, 记为

$$V_1 \oplus \cdots \oplus V_s.$$

定义 6 给出了一个由已知的线性空间构造新的线性空间的方法. 过去我们讨论过子空间的直和, 它们之间是什么关系呢?

在 $V_1 \oplus \cdots \oplus V_s$ 中, 所有形式为

$$(0, \cdots, \alpha_i, \cdots, 0),\ \alpha_i \in V_i$$

的元素显然构成一个子空间, 记为 V_i'. 容易看出, V_i' 与 V_i 同构, 而且 $V_1 \oplus \cdots \oplus V_s$ 可以表示成子空间 $V_1', \cdots, V_s'$ 的直和. 由此可见, 这里定义的直和与过去所说的直和在本质上是一回事, 不过出发点不同而已. 有时候为了区别, 过去所说的直和称为 **内直和**, 而定义 6 所说的直和称为 **外直和**.

为了下面的需要, 我们还要把定义 6 推广到无穷多个线性空间的情形. 设 $V_1, V_2, \cdots$ 是域 F 上无穷多个线性空间. 我们说一个无穷序列

$$(\alpha_1, \alpha_2, \cdots),\ \alpha_i \in V_i,\ i = 1, 2, \cdots$$

的分量几乎全为零, 如果在 $\alpha_1, \alpha_2, \cdots$ 中只有有限多个分量不为零. 考虑分量几乎全为零的无穷序列的全体, 定义

$$(\alpha_1, \alpha_2, \cdots) + (\beta_1, \beta_2, \cdots) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \cdots),$$
$$k(\alpha_1, \alpha_2, \cdots) = (k\alpha_1, k\alpha_2, \cdots).$$

显然, 这样定义的运算在所考虑的集合上是封闭的, 而且构成一线性空间.

定义 7 上面构造的线性空间称为线性空间 $V_1, V_2, \cdots$ 的 **直和**, 记为

$$V_1 \oplus V_2 \oplus \cdots = \bigoplus_{i=1}^{\infty} V_i.$$

在 $\bigoplus_{i=1}^{\infty} V_i$ 中, 除去第 i 位外全为零的序列的全体显然成一子空间, 用 V_i' 代表它. 容易证明, $V_i' \cong V_i$, 而且直和 $\bigoplus_{i=1}^{\infty} V_i$ 中的元素 α 可以唯一地表示成

$$\alpha = \alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_r},$$

其中 $\alpha_{i_j} \in V_{i_j}'$, $j = 1, \cdots, r$.

为简单起见, 我们可把 V_i' 与 V_i 等同起来. 于是直和 $\bigoplus_{i=1}^{\infty} V_i$ 中的元素 α 就可以表示成

$$\alpha = \alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_r},\ \ \alpha_{i_j} \in V_{i_j},\ j = 1, \cdots, r.$$

应该指出，“几乎全为零”的限制对于有限多个分量来说就不成为限制．因之，定义 6 与定义 7 可以统一起来．

最后再说一下线性变换的直和．设 $V_1, V_2, \cdots$，是域 F 上的线性空间，而 $\boldsymbol{A}_1, \boldsymbol{A}_2, \cdots$，分别是这些空间上的线性变换．对于直和 $\bigoplus\limits_{i=1}^{\infty} V_i$ 中的元素，我们定义变换 $\boldsymbol{A}$ 为：

$$\boldsymbol{A}(\alpha_1, \alpha_2, \cdots) = (\boldsymbol{A}_1\alpha_1, \boldsymbol{A}_2\alpha_2, \cdots),$$

显然 $\boldsymbol{A}$ 是一线性变换．线性变换 $\boldsymbol{A}$ 称为**线性变换 $\boldsymbol{A}_1, \boldsymbol{A}_2, \cdots$，的直和**，记为

$$\boldsymbol{A} = \boldsymbol{A}_1 \dotplus \boldsymbol{A}_2 \dotplus \cdots.$$

§5　张量代数

张量代数是利用张量积建立的一个与线性空间相联系的代数结构，它也是多重线性代数中的一个基本概念．

设 V 是域 F 上一 n 维线性空间．我们定义

$$\begin{aligned} &T_0(V) = F, \\ &T_r(V) = V \otimes \cdots \otimes V \ (r\text{个}), \quad r = 1, 2, \cdots \end{aligned}$$

如果 $\varepsilon_1, \cdots, \varepsilon_n$ 是 V 的一组基，那么

$$\varepsilon_{i_1} \otimes \cdots \otimes \varepsilon_{i_r}, \quad i_1, \cdots, i_r = 1, 2, \cdots, n$$

就是 $T_r(V)$ 的一组基，而 1 就是 $T_0(V)$ 的基．因之，$T_r(V)$ 的维数是 n^r，$r = 0, 1, \cdots$．

根据张量积的结合律，我们有同构映射

$$\sigma : T_r(V) \otimes T_s(V) \to T_{r-s}(V),$$

使

$$\begin{aligned} &\sigma((\alpha_1 \otimes \cdots \otimes \alpha_r) \otimes (\beta_1 \otimes \cdots \otimes \beta_s)) \\ &= \alpha_1 \otimes \cdots \otimes \alpha_r \otimes \beta_1 \otimes \cdots \otimes \beta_s, \quad r, s > 0 \end{aligned}$$

利用这个同构映射，对于 $x \in T_r(V), y \in T_s(V)$，我们定义

$$x \otimes y \in T_{r+s}(V).$$

再利用上一节所说的同构映射

$$F \otimes V \to V,$$

对于 $x \in T_r(V), k \in T_0(V)$, 我们定义

$$k \otimes x = kx, x \otimes k = kx.$$

这样, 我们就在 $T_0(V), T_1(V), \cdots, T_r(V), \cdots$ 的元素之间定义了一个乘法. 乘法的结合律是显然的, 即对于 $x \in T_r(V), y \in T_s(V), z \in T_p(V)$, 有

$$x \otimes (y \otimes z) = (x \otimes y) \otimes z,$$

其中 $r, s, p \geq 0$.

作 $T_r(V), r = 0, 1, 2, \cdots$ 这些空间的直和

$$T_0(V) \oplus T_1(V) \oplus T_2(V) \oplus \cdots$$

记为 $T(V)$. 按分配律, 上面定义的乘法立即推广到 $T(V)$ 的元素上. $T(V)$ 作为一线性空间, 它有一个加法. 不难验证, $T(V)$ 在这样的加法与乘法下成一环 (验证留给读者). 显然, 环 $T(V)$ 具有单位元素, 乘法不适合交换律. 当然, $T(V)$ 除去环的结构外, 还有一个线性空间的结构.

定义 8 如上定义的代数结构 $T(V)$ 称为线性空间 V 的 **张量代数**.

$T(V)$ 这个代数结构本身并不具有很多有趣的性质, 我们也不打算对它进行什么讨论, 但是它为以后的讨论提供了基础.

§6 交错化

从这一节开始, 我们假定域 F 的特征为 0.

设 V 为域 F 上一 n 维线性空间, $\varepsilon_1, \cdots, \varepsilon_n$ 是 V 的一组基, $T(V) = \bigoplus_{r=0}^{\infty} T_r(V)$ 是 V 的张量代数. 我们知道, 对于 $r > 0$,

$$\varepsilon_{i_1} \otimes \cdots \otimes \varepsilon_{i_r}, \quad i_1, \cdots, i_r = 1, 2, \cdots, n$$

构成 $T_r(V)$ 的一组基.

令 S_r 表示 r 个文字的对称群. 具体地说, S_r 就是由集合 $\{1, 2, \cdots, r\}$ 上全体置换组成的群. 对于任意的 $\sigma \in S_r$, 我们定义 $T_r(V)$ 的一个线性变换为

$$\sigma(\varepsilon_{i_1} \otimes \cdots \otimes \varepsilon_{i_r}) = \varepsilon_{i_{\sigma(1)}} \otimes \cdots \otimes \varepsilon_{i_{\sigma(r)}},$$

仍用 σ 表示这个线性变换. 例如, 当 $r = 3$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

于是

$$\sigma(\varepsilon_4 \otimes \varepsilon_3 \otimes \varepsilon_2) = \varepsilon_3 \otimes \varepsilon_2 \otimes \varepsilon_4,$$

也就是说，σ 是对于基向量脚标的次序作置换.

定义 9 对于 $r > 0$, 我们定义 $T_r(V)$ 的线性变换 Alt_r 为:

$$\mathrm{Alt}_r(\varepsilon_{i_1} \otimes \cdots \otimes \varepsilon_{i_r}) = \frac{1}{r!} \sum_{\sigma \in S_r} \mathrm{sgn}(\sigma)\sigma(\varepsilon_{i_1} \otimes \cdots \otimes \varepsilon_{i_r}),$$

其中 $\mathrm{sgn}(\sigma)$ 表示 σ 的符号，即

$$\mathrm{sgn}(\sigma) = \begin{cases} 1, & \text{当 } \sigma \text{ 为偶置换}, \\ -1 & \text{当 } \sigma \text{ 为奇置换}, \end{cases}$$

而 $\sum$ 对 S_r 中全体置换求和. Alt_r 称为**交错化变换**.

由线性变换 σ 的定义不难看出，对于

$$\alpha_1 \otimes \cdots \otimes \alpha_r \in T_r(V),$$

有

$$\sigma(\alpha_1 \otimes \cdots \otimes \alpha_r) = \alpha_{\sigma(1)} \otimes \cdots \otimes \alpha_{\sigma(r)}.$$

因之，我们有

$$\mathrm{Alt}_r(\alpha_1 \otimes \cdots \otimes \alpha_r) = \frac{1}{r!} \sum_{\sigma \in S_r} \mathrm{sgn}(\sigma)\sigma(\alpha_1 \otimes \cdots \otimes \alpha_r).$$

下面来讨论线性变换 Alt_r 的性质.

定理 9 对于 $\sigma \in S_r$, 我们有

$$\mathrm{Alt}_r \cdot \sigma = \sigma \cdot \mathrm{Alt}_r = \mathrm{sgn}(\sigma)\mathrm{Alt}_r.$$

证明 因为 $T_r(V)$ 中元素全可以表成形式为

$$\alpha_1 \otimes \cdots \otimes \alpha_r$$

的元素之和. 所以在讨论线性变换的性质时，我们只需要考察线性变换在这种元素上的作用就行了.

$$\begin{aligned} &\mathrm{Alt}_r \cdot \sigma(\alpha_1 \otimes \cdots \otimes \alpha_r) \\ &= \frac{1}{r!} \sum_{\tau \in S_r} \mathrm{sgn}(\tau)\tau \cdot \sigma(\alpha_1 \otimes \cdots \otimes \alpha_r). \end{aligned}$$

我们知道，$(\mathrm{sgn}(\tau))^2=1$，对所有的 $\tau\in S_r$；而且当 τ 取遍 S_r 中元素时，$\tau\sigma$ 也取遍 S_r 中元素．由此即得

$$\begin{aligned}
&\mathrm{Alt}_r\cdot\sigma(\alpha_1\otimes\cdots\otimes\alpha_r)\\
&=\frac{1}{r!}\mathrm{sgn}(\sigma)\sum_{\tau\in S_r}\mathrm{sgn}(\tau)\mathrm{sgn}(\sigma)\tau(\sigma(\alpha_1\otimes\cdots\otimes\alpha_r))\\
&=\mathrm{sgn}(\sigma)\frac{1}{r!}\sum_{\tau\in S_r}\mathrm{sgn}(\tau\sigma)(\tau\sigma)(\alpha_1\otimes\cdots\otimes\alpha_r)\\
&=\mathrm{sgn}(\sigma)\frac{1}{r!}\sum_{\tau\in S_r}\mathrm{sgn}(\tau)\tau(\alpha_1\otimes\cdots\otimes\alpha_r)\\
&=\mathrm{sgn}(\sigma)\mathrm{Alt}_r(\alpha_1\otimes\cdots\otimes\alpha_r),
\end{aligned}$$

于是

$$\mathrm{Alt}_r\cdot\sigma=\mathrm{sgn}(\sigma)\mathrm{Alt}_r.$$

同样可证

$$\sigma\cdot\mathrm{Alt}_r=\mathrm{sgn}(\sigma)\mathrm{Alt}_r.$$

定理告诉我们，Alt_r 与 σ 是可交换的． □

推论 1 $\mathrm{Alt}_r\cdot\mathrm{Alt}_r=\mathrm{Alt}_r$.

证明

$$\begin{aligned}
&\mathrm{Alt}_r\cdot\mathrm{Alt}_r(\alpha_1\otimes\cdots\otimes\alpha_r)\\
&=\mathrm{Alt}_r\left(\frac{1}{r!}\sum_{\sigma\in S_r}\mathrm{sgn}(\sigma)\sigma(\alpha_1\otimes\cdots\otimes\alpha_r)\right)\\
&=\frac{1}{r!}\sum_{\sigma\in S_r}\mathrm{sgn}(\sigma)\mathrm{Alt}_r\cdot\sigma(\alpha_1\otimes\cdots\otimes\alpha_r)\\
&=\frac{1}{r!}\sum_{\sigma\in S_r}(\mathrm{sgn}(\sigma))^2\mathrm{Alt}_r(\alpha_1\otimes\cdots\otimes\alpha_r)\\
&=\mathrm{Alt}_r(\alpha_1\otimes\cdots\otimes\alpha_r).
\end{aligned}$$

这里是因为 S_r 有 $r!$ 个元素，所以，

$$\sum_{\sigma\in S_r}(\mathrm{sgn}(\sigma))^2=\sum_{\sigma\in S_r}1=r!.$$

这就证明了

$$\mathrm{Alt}_r\cdot\mathrm{Alt}_r=\mathrm{Alt}_r.\quad\square$$

由此可知，Alt_r是一个幂等元素．

推论 2 当 $r>n$ 时，$\mathrm{Alt}_r=0$.

证明 设 $\varepsilon_1,\cdots,\varepsilon_n$ 是线性空间 V 的一组基. 我们知道, $T_r(r)$ 的一组基为

$$\varepsilon_{i_1}\otimes\cdots\otimes\varepsilon_{i_r},\quad i_1,\cdots,i_r=1,2,\cdots,n.$$

因为 $r>n$, 所以不论脚标怎样取, 在向量 $\varepsilon_{i_1},\cdots,\varepsilon_{i_r}$ 中总是有两个是一样的. 譬如说, $i_j=i_k$. 令 $\sigma=(jk)$. 于是

$$\varepsilon_{i_1}\otimes\cdots\otimes\varepsilon_{i_r}=\sigma(\varepsilon_{i_1}\otimes\cdots\otimes\varepsilon_{i_r}).$$

根据定理 9, 有

$$\begin{aligned}&\mathrm{Alt}_r(\varepsilon_{i_1}\otimes\cdots\otimes\varepsilon_{i_r})\\&\quad=\mathrm{Alt}_r\sigma(\varepsilon_{i_1}\otimes\cdots\otimes\varepsilon_{i_r})\\&\quad=\mathrm{sgn}(\sigma)\mathrm{Alt}_r(\varepsilon_{i_1}\otimes\cdots\otimes\varepsilon_{i_r})\\&\quad=-\mathrm{Alt}_r(\varepsilon_{i_1}\otimes\cdots\otimes\varepsilon_{i_r}),\end{aligned}$$

由此即得

$$\mathrm{Alt}_r(\varepsilon_{i_1}\otimes\cdots\otimes\varepsilon_{i_r})=0.$$

Alt_r 把每个基向量变成零, 当然 $\mathrm{Alt}_r=0$. □

这就是说, 当 $r>n$, 在 $T_r(V)$ 上 Alt_r 是零变换.

推论 3 对于任意的 $x\in T_r(V), y\in T_s(V)$, 有

$$\mathrm{Alt}_{r+s}(x\otimes y)=(-1)^{rs}\mathrm{Alt}_{r+s}(y\otimes x).$$

证明 设 $x=\alpha_1\otimes\cdots\otimes\alpha_r, y=\beta_1\otimes\cdots\otimes\beta_n$. 取

$$\sigma=\begin{pmatrix}1&2&\cdots&s&s+1&\cdots&r+s\\r+1&r+2&\cdots&r+s&1&\cdots&r\end{pmatrix},$$

显然有

$$\sigma(x\otimes y)=y\otimes x.$$

由于 $T_r(V)$ 的元素全是上面这种形式元素之和, $T_s(V)$ 也如此, 而 σ 是线性变换, 所以对于任意的 $x\in T_r(V), y\in T_s(V)$ 也都有

$$\sigma(x\otimes y)=y\otimes x,$$

简单计算即得

$$\mathrm{sgn}(\sigma)=(-1)^{rs},$$

根据定理立即推出所要的结论. □

定义 10 $T_r(V)$ 中元素 x $(r>0)$ 称为**反对称**的，如果对于所有的 $\sigma\in S_r$ 适合

$$\sigma(x)=\mathrm{sgn}(\sigma)x.$$

定理 10 设 $x\in T_r(V)$ $(r>0)$. x 是反对称的当且仅当 $\mathrm{Alt}_r x=x$.

证明 如果 x 反对称，即 $\sigma(x)=\mathrm{sgn}(\sigma)x$, 那么

$$\begin{aligned}\mathrm{Alt}_r x&=\frac{1}{r!}\sum_{\sigma\in S_r}\mathrm{sgn}(\sigma)\sigma(x)\\&=\frac{1}{r!}\sum_{\sigma\in S_r}(\mathrm{sgn}(\sigma))^2x=x.\end{aligned}$$

反过来，如果 $\mathrm{Alt}_r x=x$, 那么由定理 9 即得

$$\sigma(x)=\sigma\mathrm{Alt}_r(x)=\mathrm{sgn}(\sigma)\mathrm{Alt}_r x=\mathrm{sgn}(\sigma)x.\quad\square$$

定义 11 $E_0(V)=T_0(V)=F$,

对于 $r>0, E_r(V)=\mathrm{Alt}_rT_r(V)$.

$E_r(V)$ 就是 Alt_r 的象空间. 由上面的讨论可知，当 $r>n$ 时，$E_r(V)$ 为零空间.

推论 设 $x\in T_r(V)$ $(r>0)$. x 是反对称的当且仅当 $x\in E_r(V)$.

证明 由 Alt_r 的幂等性可知，如果 $x\in E_r(V)$, 那么 $\mathrm{Alt}_r x=x, x$ 即反对称.

如果 x 反对称，那么 $x=\mathrm{Alt}_r x\in E_r(V)$. □

由 Alt_r 的定义可知，当 $r=1$ 时，Alt_r 就是恒等变换. 以下我们约定 Alt_0 就是 F 上的恒等变换. 这个约定与定义 11 是一致的.

定理 11 对于 $x\in T_r(V), y\in T_s(V), z\in T_p(V)$, 我们有

$$\begin{aligned}&\mathrm{Alt}_{r+s+p}(\mathrm{Alt}_{r+s}(x\otimes y)\otimes z)\\&\quad=\mathrm{Alt}_{r+s+p}(x\otimes\mathrm{Alt}_{s+p}(y\otimes z))\\&\quad=\mathrm{Alt}_{r+s+p}(x\otimes y\otimes z).\end{aligned}$$

证明 以下证明只考虑 $r,s,p>0$ 的情形，其余情形留给读者.

我们先来证明

$$\mathrm{Alt}_{r+s+p}(\mathrm{Alt}_{r+s}(x\otimes y)\otimes z)=\mathrm{Alt}_{r+s+p}(x\otimes y\otimes z).$$

对于 $\sigma\in S_{r+s}$, 我们定义 $\sigma'\in S_{r+s+p}, \sigma'$ 在 $(1,2,\cdots,r+s)$ 上的作用与 σ 相同，而保持 $\{r+s+1,\cdots,r+s+p\}$ 中每个元素不动. 显然，映射 $\sigma\mapsto\sigma'$ 是

S_{r+s} 到 S_{r+s+p} 的一个单一同态，而且 $\mathrm{sgn}(\sigma)=\mathrm{sgn}(\sigma')$.

$$\begin{aligned}
&\mathrm{Alt}_{r+s+p}(\mathrm{Alt}_{r+s}(x\otimes y)\otimes z)\\
&=\mathrm{Alt}_{r+s+p}\left(\frac{1}{(r+s)!}\left(\sum_{\sigma\in S_{r+s}}\mathrm{sgn}(\sigma)\sigma(x\otimes y)\right)\otimes z\right)\\
&=\mathrm{Alt}_{r+s+p}\left(\frac{1}{(r+s)!}\sum_{\sigma\in S_{r+s}}\mathrm{sgn}(\sigma)\sigma(x\otimes y)\otimes z\right)\\
&=\mathrm{Alt}_{r+s+p}\left(\frac{1}{(r+s)!}\sum_{\sigma\in S_{r+s}}\mathrm{sgn}(\sigma')\sigma'(x\otimes y\otimes z)\right)\\
&=\frac{1}{(r+s)!}\sum_{\sigma\in S_{r+s}}\mathrm{sgn}(\sigma')\mathrm{Alt}_{r+s+p}\sigma'(x\otimes y\otimes z)\\
&=\mathrm{Alt}_{r+s+p}(x\otimes y\otimes z).
\end{aligned}$$

至于第 2 个等式的证明，我们只要改变一下置换群的映射就行了．对于 $\sigma\in S_{s+p}$，我们定义 $\sigma'\in S_{r+s+p}$，它保持 $\{1,\cdots,r\}$ 中每个元素不动，而在 $\{r+1,\cdots,r+s+p\}$ 上的作用按顺序与 σ 在 $\{1,\cdots,s+p\}$ 上的作用相同．显然，$\sigma\mapsto\sigma'$ 也是 S_{s+p} 到 S_{r+s+p} 的一个单一同态，且 $\mathrm{sgn}(\sigma)=\mathrm{sgn}(\sigma')$．证明的其余步骤完全一样． □

§7 外代数

上面对于每个 $T_r(V)$ 我们定义了交错化变换 Alt_r，作它们的直和

$$\mathrm{Alt}=\mathrm{Alt}_0+\mathrm{Alt}_1+\cdots,$$

它是 $T(V)$ 上的线性变换．根据以上的讨论我们有

$$\mathrm{Alt}T(V)=E_0(V)+E_1(V)+\cdots+E_n(V),$$

用 $E(V)$ 表示这个线性空间．

在 $E(V)$ 上我们来定义一个新的乘法．

定义 12 对于 $x,y\in E(V)$，令

$$x\wedge y=\mathrm{Alt}(x\otimes y),$$

$x\wedge y$ 称为 x,y 的 **外乘积**.

设

$$x=x_0+x_1+\cdots+x_n,y=y_0+y_1+\cdots+y_n,$$

其中 $x_i, y_i \in E_i(V)$, $i=0,1,\cdots,n$. 按定义,

$$x\wedge y=\mathrm{Alt}(x\otimes y)=\mathrm{Alt}\left(\sum_{i=0}^{n}\sum_{j=0}^{n}x_i\otimes y_j\right)$$
$$=\sum_{i=0}^{n}\sum_{j=0}^{n}\mathrm{Alt}_{i+j}(x_i\otimes y_j).$$

对于 $k\in E_0(V), x\in E(V)$, 显然有

$$k\wedge x=x\wedge k=kx,$$

因之, $1\in E_0(V)$ 就是这个乘法的单位元素.

由定理 9 推论 2, 对于 $x\in E_r(V), y\in E_s(V)$, 如果 $r+s>n$, 那么 $x\wedge y=0$.

由定理 11, 我们有

$$x\wedge(y\wedge z)=(x\wedge y)\wedge z,$$

即外乘适合结合律.

由定理 9 推论 3, 对于 $x\in E_r(V), y\in E_s(V)$, 我们有

$$x\wedge y=(-1)^{rs}y\wedge x.$$

特别地, 对于 $\alpha,\beta\in V=E_1(V)$ 有

$$\alpha\wedge\beta=-\beta\wedge\alpha,$$

由此即得, 对于 $\alpha\in V$, 有

$$\alpha\wedge\alpha=0.$$

因为 $T_r(V)$ 的元素全可以表示成形式为

$$\alpha_1\otimes\cdots\otimes\alpha_r$$

的元素的有限和, 而

$$\mathrm{Alt}(\alpha_1\otimes\cdots\otimes\alpha_r)=\alpha_1\wedge\cdots\wedge\alpha_r,$$

所以 $E_r(V)$ 的元素全可以表示成形式为

$$\alpha_1\wedge\cdots\wedge\alpha_r\ (\alpha_1,\cdots,\alpha_r\in V)$$

的元素的有限和.

定义 13 $E(V)$ 在数量乘法、加法与外乘这些运算下所成的代数结构称为线性空间 V 的 **外代数** 或 **格拉斯曼** (Grassmann) **代数**.

撇开数量乘法, $E(V)$ 是一具有单位元素的环, 这个环有零因子.

定理 12 设 V 为域 F 上一 n 维线性空间, $\varepsilon_1,\cdots,\varepsilon_n$ 是 V 的一组基. 于是

1) $E_0(V)$ 的维数是 1, 对于 $0<r\leq n,\varepsilon_{i_1}\wedge\cdots\wedge\varepsilon_{i_r}$, 其中 $1\leq i_1<i_2<\cdots<i_r\leq n$, 构成 $E_r(V)$ 的一组基, 从而 $E_r(V)$ 的维数是 $\begin{pmatrix} n \\ r \end{pmatrix}$.

2) $E(V)$ 的维数是 2^n.

证明 这里只需要证明, 对于 $0<r\leq n,\varepsilon_{i_1}\wedge\cdots\wedge\varepsilon_{i_r}$, 其中 $1\leq i_1<i_2<\cdots<i_r\leq n$, 构成 $E_r(V)$ 的一组基就行了, 其余的都是这个结论的简单推论.

上面已经看到, $E_r(V)$ 中元素全可以表示成 $\alpha_1\wedge\cdots\wedge\alpha_r$ 这种元素的有限和, 因而都可以表成

$$\varepsilon_{i_1}\wedge\cdots\wedge\varepsilon_{i_r},\quad i_1,\cdots,i_r=1,\cdots,n$$

这些元素的线性组合. 因为 $\varepsilon_i\wedge\varepsilon_j=-\varepsilon_j\wedge\varepsilon_i$, 所以 $\varepsilon_{i_1},\cdots,\varepsilon_{i_r}$ 这些元素的外乘积, 当次序不同时, 最多相差一个正负号, 由此可知, $E_r(V)$ 的元素一定可以被

$$\varepsilon_{i_1}\wedge\cdots\wedge\varepsilon_{i_r},\quad 1\leq i_1<i_2<\cdots<i_r\leq n$$

这些元素线性表出. 下面来证它们的线性无关性. 我们知道,

$$\begin{aligned}\varepsilon_{i_1}\wedge\cdots\wedge\varepsilon_{i_r}&=\mathrm{Alt}_r(\varepsilon_{i_1}\otimes\cdots\otimes\varepsilon_{i_r})\\&=\frac{1}{r!}\sum_{\sigma\in S_r}\mathrm{sgn}(\sigma)\sigma(\varepsilon_{i_1}\otimes\cdots\otimes\varepsilon_{i_r}).\end{aligned}$$

如果 $(i_1,\cdots,i_r)\neq(j_1,\cdots,j_r)$, 其中 $j_1,\cdots,j_r$ 也适合条件 $1\leq j_1<j_2<\cdots<j_r\leq n$, 那么对于任意 $\sigma,\tau\in S_r$, 有

$$\sigma(\varepsilon_{i_1}\otimes\cdots\otimes\varepsilon_{i_r})\neq\tau(\varepsilon_{j_1}\otimes\cdots\otimes\varepsilon_{j_r}),$$

这就是说, 在表示成 $T_r(V)$ 中一组基元素的线性组合时, 在 $\varepsilon_{i_1}\wedge\cdots\wedge\varepsilon_{i_r}$, $1\leq i_1<i_2<\cdots<i_r\leq n$, 的不同元素中出现的基元素全不相同, 因而它们线性无关. □

定义 14 $E_r(V)$ 中的元素称为 r-**向量**.

下面我们将建立 r- 向量与 V 中 r 维子空间的联系. 在这之前先证明

定理 13 设 $\alpha_1,\cdots,\alpha_r\in V$. $\alpha_1\wedge\cdots\wedge\alpha_r=0$ 当且仅当 $\alpha_1,\cdots,\alpha_r$ 线性相关.

证明 无妨假定 $r>1$. 因为 $r=1$ 的情形是显然的.

如果 $\alpha_1,\cdots,\alpha_r$ 线性相关，譬如说，α_r 可以表成 $\alpha_1,\cdots,\alpha_{r-1}$ 的线性组合，

$$\alpha_r = b_1\alpha_1 + \cdots + b_{r-1}\alpha_{r-1},$$

那么有

$$\begin{aligned}&\alpha_1\wedge\cdots\wedge\alpha_{r-1}\wedge\alpha_r\\&\quad=\alpha_1\wedge\cdots\wedge\alpha_{r-1}\wedge(b_1\alpha_1+\cdots+b_{r-1}\alpha_{r-1})\\&\quad=\sum_{i=1}^{r-1}b_i\alpha_1\wedge\cdots\wedge\alpha_{r-1}\wedge\alpha_i=0.\end{aligned}$$

反过来，如果 $\alpha_1,\cdots,\alpha_r$ 线性无关，那么它们可以扩充成 V 的一组基，譬如说，

$$\alpha_1,\cdots,\alpha_r,\beta_1,\cdots,\beta_{n-r}$$

是 V 的一组基. 由定理 12, $\alpha_1\wedge\cdots\wedge\alpha_r$ 是 $E_r(V)$ 的一组基中的一个元素，从而

$$\alpha_1\wedge\cdots\wedge\alpha_r\neq 0.\quad\square$$

在三维欧氏空间中，向量之间可以定义 × 乘. 如果 α,β 生成一个二维子空间，那么

$$\alpha\times\beta$$

就是这个二维子空间的一个法向量. 法向量 $\alpha\times\beta$ 不但唯一决定这个二维子空间，而且还给出这个二维子空间一个定向. 如果再考虑到向量的度量性质，那么向量 $\alpha\times\beta$ 的长度就等于以 α,β 为边的平行四边形的面积，而向量 $\alpha\times\beta$ 本身就可以认为是给出了这个平行四边形的定向面积. 当 $n>3$ 时，在 n 维空间中，我们不再有 × 乘的概念. 而外乘积正是 × 乘的一个推广.

定理 14 设 V 是域 F 上一 n 维线性空间，W 是 V 的一个子空间，$\eta_1,\cdots,\eta_r$ 是 W 的一组基. 于是 r- 向量 $x=\eta_1\wedge\cdots\wedge\eta_r$ 除一非零常数倍外，被子空间 W 所决定，且

$$W=\{\alpha\in V\,|\,\alpha\wedge x=0\}.$$

证明 设 $\zeta_1,\cdots,\zeta_r$ 是 W 的另一组基. 于是我们有

$$\begin{aligned}\zeta_1&=c_{11}\eta_1+\cdots+c_{1r}\eta_r,\\&\cdots\cdots\cdots\cdots\\\zeta_r&=c_{r1}\eta_1+\cdots+c_{rr}\eta_r,\end{aligned}$$

其中 $|c_{ij}|\neq 0$. 直接计算即得

$$\begin{aligned}\zeta_1\wedge\cdots\wedge\zeta_r&=(c_{11}\eta_1+\cdots+c_{1r}\eta_r)\wedge\cdots\wedge(c_{r1}\eta_1+\cdots+c_{rr}\eta_r)\\&=|c_{ij}|\eta_1\wedge\cdots\wedge\eta_r.\end{aligned}$$

这就证明了，除去可以差一非零倍数外，r- 向量 $\eta_1\wedge\cdots\wedge\eta_r$ 被 W 唯一决定，而与基的选择无关. 由定理 13 立即推出

$$W=\{\alpha\in V\,|\,\alpha\wedge x=0\}.\quad\square$$

定理 14 表明，r- 向量 $\eta_1\wedge\cdots\wedge\eta_r$ 完全决定了子空间 W. 如果 V 是一欧氏空间，那么按适当的方式在 $E_r(V)$ 中可以定义内积. 于是 r- 向量 $\eta_1\wedge\cdots\wedge\eta_r$ 不但决定了子空间 W, 而且给出了 W 的一个定向. r- 向量 $\eta_1\wedge\cdots\wedge\eta_r$ 的长度就等于由 $\eta_1,\cdots,\eta_r$ 张成的 r 维平行体的体积. 这些就不细说了.

如果在 n 维线性空间 V 中取定一组基

$$\varepsilon_1,\cdots,\varepsilon_n,$$

那么 $\varepsilon_{i_1}\wedge\cdots\wedge\varepsilon_{i_r}$, $1\leq i_1<\cdots<i_r\leq n$ 就是 $E_r(V)$ 的一组基. 对于 r 维子空间 W, 取一组基 $\eta_1,\cdots,\eta_r$, 我们有

$$\eta_1\wedge\cdots\wedge\eta_r=\sum b_{i_1\cdots i_r}\varepsilon_{i_1}\wedge\cdots\wedge\varepsilon_{i_r},$$

其中 $1\leq i_1<\cdots<i_r\leq n$. 把基向量 $\varepsilon_{i_1}\wedge\cdots\wedge\varepsilon_{i_r}$ 按一定顺序排好，数组

$$b_{i_1\cdots i_r},\quad 1\leq i_1<\cdots<i_r\leq n$$

就称为子空间 W 的 **普吕克** (Plücker) **坐标**. 上面的讨论表明，在取定 V 的一组基之后，子空间完全被它的普吕克坐标决定，而普吕克坐标可以相差一个非零倍数.

因为 r 维子空间 W 的普吕克坐标可以相差一个非零常数，所以它可以看作 C_n^r-1 维射影空间中的一个点. n 维线性空间中全体 r 维子空间可以看作是 C_n^r-1 维射影空间中的一个子集合. 可以证明，这个子集合是一代数流形，通常称为 **格拉斯曼流形**.

§8 $E(V)$ 的线性变换与对偶

设 V 是域 F 上一 n 维线性空间，$\boldsymbol{A}$ 是线性空间 V 的一个线性变换. 我们已经定义过线性变换的张量积，即 $\boldsymbol{A}\otimes\cdots\otimes\boldsymbol{A}$($r$ 个) 是 $T_r(V)$ 到自身的线性变换. 我们来证明，$E_r(V)$ 是这个线性变换的不变子空间. 事实上，对于

$$\alpha_1\otimes\cdots\otimes\alpha_r\in T_r(V),$$

我们有

$$\begin{aligned}&(\boldsymbol{A}\otimes\cdots\otimes\boldsymbol{A})\mathrm{Alt}_r(\alpha_1\otimes\cdots\otimes\alpha_r)\\&=(\boldsymbol{A}\otimes\cdots\otimes\boldsymbol{A})\frac{1}{r!}\sum_{\sigma\in S_r}\mathrm{sgn}(\sigma)\sigma(\alpha_1\otimes\cdots\otimes\alpha_r)\\&=\frac{1}{r!}\sum_{\sigma\in S_r}\mathrm{sgn}(\sigma)\sigma(\boldsymbol{A}\alpha_1\otimes\cdots\otimes\boldsymbol{A}\alpha_r)\\&=\mathrm{Alt}_r(\boldsymbol{A}\otimes\cdots\otimes\boldsymbol{A})(\alpha_1\otimes\cdots\otimes\alpha_r).\end{aligned}$$

这就是说，在 $T_r(V)$ 上，$(\boldsymbol{A}\otimes\cdots\otimes\boldsymbol{A})$ 与 Alt_r 是可交换的，因而 Alt_r 的象空间 $E_r(V)$ 是 $\boldsymbol{A}\otimes\cdots\otimes\boldsymbol{A}$ 的不变子空间.

限制 $\boldsymbol{A}\otimes\cdots\otimes\boldsymbol{A}$ 在 $E_r(V)$ 所得到的线性变换称为由 A 在 $E_r(V)$ 上诱导出的线性变换. 这个线性变换记为

$$\boldsymbol{A}\wedge\cdots\wedge\boldsymbol{A}\ (r\ \text{个}).$$

由定义以及线性变换的张量积的性质立即得出：对于线性变换 $\boldsymbol{A},\boldsymbol{B}:V\to V$, 对于单位变换 $\boldsymbol{E}$ 有

1. $(\boldsymbol{A}\wedge\cdots\wedge\boldsymbol{A})(\boldsymbol{B}\wedge\cdots\wedge\boldsymbol{B})=(\boldsymbol{AB}\wedge\cdots\wedge\boldsymbol{AB})$.
2. $\boldsymbol{E}\wedge\cdots\wedge\boldsymbol{E}$ 是 $E_r(V)$ 上的单位变换.
3. 如果 $\boldsymbol{A}$ 可逆，那么 $\boldsymbol{A}\wedge\cdots\wedge\boldsymbol{A}$ 也可逆，且

$$(\boldsymbol{A}\wedge\cdots\wedge\boldsymbol{A})^{-1}=\boldsymbol{A}^{-1}\wedge\cdots\wedge\boldsymbol{A}^{-1}.$$

对于 V 的对偶空间 V^* 我们当然也可以定义 $T_r(V^*)$ 与 $E_r(V^*)$, 下面来建立 $E_r(V^*)$ 到 $E_r(V)^*$ 的一个同构映射.

设 $f_1,\cdots,f_r\in V^*$, 定义

$$(f_1\otimes\cdots\otimes f_r)(\alpha_1\otimes\cdots\otimes\alpha_r)=f_1(\alpha_1)\cdots f_r(\alpha_r),$$

我们知道，这就给出了 $T_r(V^*)$ 到 $T_r(V)^*$ 的一个同构映射. 在这个映射下,

$$\begin{aligned}&f_1\wedge\cdots\wedge f_r(\alpha_1\wedge\cdots\wedge\alpha_r)\\&=f_1\wedge\cdots\wedge f_r\left(\frac{1}{r!}\sum_{\sigma\in S_r}\mathrm{sgn}(\sigma)\sigma(\alpha_1\otimes\cdots\otimes\alpha_r)\right)\\&=\frac{1}{r!}\sum_{\sigma\in S_r}\mathrm{sgn}(\sigma)f_1\wedge\cdots\wedge f_r(\alpha_{\sigma(1)}\otimes\cdots\otimes\alpha_{\sigma(r)})\\&=\frac{1}{r!}\sum_{\sigma\in S_r}\mathrm{sgn}(\sigma)\cdot\frac{1}{r!}\sum_{\tau\in S_r}\mathrm{sgn}(\tau)f_{\tau(1)}\otimes\cdots\otimes f_{\tau(r)}\cdot(\alpha_{\sigma(1)}\otimes\cdots\otimes\alpha_{\sigma(r)})\\&=\frac{1}{r!}\sum_{\sigma\in S_r}\mathrm{sgn}(\sigma)\cdot\frac{1}{r!}\sum_{\tau\in S_r}\mathrm{sgn}(\tau)f_{\tau(1)}(\alpha_{\sigma(1)})\cdots f_{\tau(r)}(\alpha_{\sigma(r)}).\end{aligned}$$

不难看出,

$$\sum_{\tau\in S_r}\operatorname{sgn}(\tau)f_{\tau(1)}(\alpha_{\sigma(1)})\cdots f_{\tau(r)}(\alpha_{\sigma(r)})=|f_i(\alpha_{\sigma(j)})|=\operatorname{sgn}(\sigma)|f_i(\alpha_j)|,$$

于是

$$\begin{aligned}&f_1\wedge\cdots\wedge f_r(\alpha_1\wedge\cdots\wedge\alpha_r)\\&=\frac{1}{(r!)^2}\sum_{\sigma\in S_r}\operatorname{sgn}(\sigma)^2|f_i(\alpha_j)|\\&=\frac{1}{r!}|f_i(\alpha_j)|.\end{aligned}$$

在 V^* 中取 $\varepsilon_1,\cdots,\varepsilon_n$ 的对偶基 $f_1,\cdots,f_n$, 即

$$f_i(\varepsilon_j)=\delta_{ij},\quad i,j=1,\cdots,n.$$

我们知道, $f_{i_1}\wedge\cdots\wedge f_{i_r}$, $1\le i_1<\cdots<i_r\le n$ 是 $E_r(V^*)$ 的一组基, 根据以上计算, 我们有

$$f_{i_1}\wedge\cdots\wedge f_{i_r}(\varepsilon_{j_1}\wedge\cdots\wedge\varepsilon_{j_r})=\begin{cases}\dfrac{1}{r!}, & 当\ (i_1,\cdots,i_r)=(j_1,\cdots,j_r),\\ 0, & 当\ (i_1,\cdots,i_r)\neq(j_1,\cdots,j_r).\end{cases}$$

这就是说, 在上面这个同构映射下, $E_r(V^*)$ 的基 $f_{i_1}\wedge\cdots\wedge f_{i_r}$, $1\le i_1<\cdots<i_r\le n$, 映射到 $E_r(V)$ 的基 $\varepsilon_{j_1}\wedge\cdots\wedge\varepsilon_{j_r}$, $1\le j_1<\cdots<j_r\le n$, 的对偶基, 因而给出了 $E_r(V^*)$ 到 $E_r(V)^*$ 的一个同构映射. 以后我们常常按这个同构映射把 $E_r(V^*)$ 与 $E_r(V)^*$ 等同起来.

向量的外乘积与线性空间的外代数在现代分析与微分几何中已经是必不可少的工具. 这里只是给出它们的基本的代数性质, 至于如何应用在其它有关课程中将会谈到.

习 题

1. 设 V,W 是域 F 上的线性空间. 我们用

$$\operatorname{Hom}(V,W)$$

代表全体由 V 到 W 的线性变换所成的集合, 在 $\operatorname{Hom}(V,W)$ 上, 我们定义运算如下: 对于 $\boldsymbol{A},\boldsymbol{B}\in\operatorname{Hom}(V,W)$, $k\in F$,

$$(\boldsymbol{A}+\boldsymbol{B})\alpha=\boldsymbol{A}\alpha+\boldsymbol{B}\alpha,$$
$$(k\boldsymbol{A})\alpha=k(\boldsymbol{A}\alpha),\ \alpha\in V.$$

证明 $\mathrm{Hom}(V,W)$ 在这样的运算下成一线性空间.

2. 设 V,W 是域 F 上的线性空间，维数分别为 n,m，而 $\varepsilon_1,\cdots,\varepsilon_n$ 与 $\eta_1,\cdots,\eta_m$ 分别是 V 与 W 的基. 对于 $\boldsymbol{A}\in\mathrm{Hom}(V,W)$，有

$$\begin{aligned}\boldsymbol{A}\varepsilon_1&=a_{11}\eta_1+\cdots+a_{m1}\eta_m,\\&\cdots\cdots\cdots\cdots\cdots\cdots\\\boldsymbol{A}\varepsilon_n&=a_{1n}\eta_1+\cdots+a_{mn}\eta_m.\end{aligned}$$

我们称矩阵

$$A=\begin{pmatrix}a_{11}&\cdots&a_{1n}\\\cdots&\cdots&\cdots\\a_{m1}&\cdots&a_{mn}\end{pmatrix}$$

为线性变换 $\boldsymbol{A}$ 在这两组基下的矩阵. 证明：这个对应是由线性空间 $\mathrm{Hom}(V,W)$ 到全体 $m\times n$ 矩阵组成的线性空间的一个同构映射.

3. 设线性空间 V,W 的维数分别是 n,m，求 $\mathrm{Hom}(V,W)$ 的维数.

4. 设 $\varepsilon_1,\cdots,\varepsilon_n,\eta_1,\cdots,\eta_m$ 分别是线性空间 V,W 的基，线性变换 $\boldsymbol{A}\in\mathrm{Hom}(V,W)$ 在这两组基下的矩阵为 A. 作基变换

$$\begin{aligned}(\varepsilon_1',\cdots,\varepsilon_n')&=(\varepsilon_1,\cdots,\varepsilon_n)P,\\(\eta_1',\cdots,\eta_m')&=(\eta_1,\cdots,\eta_m)Q.\end{aligned}$$

求线性变换 $\boldsymbol{A}$ 在新基下的矩阵.

5. 设线性空间 V 与 W 的维数分别是 n 与 m，$\boldsymbol{A}\in\mathrm{Hom}(V,W)$. 证明：在 V 与 W 中可以分别取基 $\varepsilon_1,\cdots,\varepsilon_n$ 与 $\eta_1,\cdots,\eta_m$ 使

$$\begin{aligned}\boldsymbol{A}\varepsilon_i&=\eta_i,\quad i=1,\cdots,r,\\\boldsymbol{A}\varepsilon_j&=0,\quad j=r+1,\cdots,n.\end{aligned}$$

叙述与之联系的关于矩阵的结果.

6. 设 V 为域 F 上一 n 维线性空间，V^* 是 V 的对偶空间. 对于子空间 $W\subset V$ 定义

$$\mathrm{ann}(W)=\{f\in V^*\mid f(\alpha)=0\text{ 对 }\alpha\in W\}.$$

因为 V 可以看作 V^* 的对偶，所以对于子空间 $U\subset V^*$，同样可以定义 $\mathrm{ann}(U)$. 证明

(i) $\mathrm{d}(\mathrm{ann}(W))=n-\mathrm{d}(W)$，

(ii) $\mathrm{ann}(\mathrm{ann}(W))=W$，

(iii) 如果 $\mathrm{d}(W)<n$，那么有非零的 $f\in V^*$，使 $f(\alpha)=0$ 对所有的 $\alpha\in W$.

($\mathrm{d}(X)$ 表示 X 的维数.)

7. 设 V 为域 F 上的一 n 维线性空间，V^* 为 V 的对偶空间，$\varepsilon_1,\cdots,\varepsilon_n$ 为 V 的一组基，$f_1,\cdots,f_n$ 为对偶基. 如果 $\eta_1,\cdots,\eta_n$ 是 V 的另一组基，

$$(\eta_1,\cdots,\eta_n)=(\varepsilon_1,\cdots,\varepsilon_n)C.$$

求由 $f_1,\cdots,f_n$ 到 $\eta_1,\cdots,\eta_n$ 的对偶基的过渡矩阵.

8. 设 V 是域 F 上一 n 维线性空间， V^* 为 V 的对偶空间， $\varepsilon_1,\cdots,\varepsilon_n$ 为 V 的一组基， $f_1,\cdots,f_n$ 为对偶基. 定义同构映射 $\varphi:V\to V^*$ 为

$$\varphi(\varepsilon_i)=f_i,\quad i=1,\cdots,n.$$

证明：随着基的不同这样定义的同构映射一般是不同的.

9. 设 V,W 是域 F 上的有限维线性空间， V^*,W^* 分别是它们的对偶空间.

(i) 对于给定的 $\boldsymbol{A}\in \mathrm{Hom}(V,W)$, 对于任意的 $g\in W^*$, 证明存在唯一的 $f\in V^*$, 使

$$f(\alpha)=g(\boldsymbol{A}\alpha),\quad \alpha\in V.$$

(ii) 证明，上面定义的映射 $g\mapsto f$ 是 W^* 到 V^* 的一个线性变换. 这个线性变换记为 $\boldsymbol{A}^*$.

(iii) 证明 $\boldsymbol{A}\mapsto \boldsymbol{A}^*$ 是 $\mathrm{Hom}(V,W)$ 到 $\mathrm{Hom}(W^*,V^*)$ 的一个线性变换.

(iv) 在对偶基下， $\boldsymbol{A}$ 与 $\boldsymbol{A}^*$ 的矩阵有什么关系?

10. 设 V,W 是域 F 上两个有限维线性空间， $f(\alpha,\beta)\in P(V,W)$. 令

$$V^0=\{\alpha\in V\mid f(\alpha,\beta)=0\text{ 对所有的 }\beta\in W\},$$
$$W^0=\{\beta\in W\mid f(\alpha,\beta)=0\text{ 对所有的 }\alpha\in V\}.$$

(i) 证明 V^0,W^0 是子空间.

(ii) 如果 $V^0=\{0\}$, 证明 $\mathrm{d}(V)\le \mathrm{d}(W)$; 同样，如果 $W^0=\{0\}$, 那么 $\mathrm{d}(W)\le\mathrm{d}(V)$.

(iii) 对于商空间 V/V^0 与 W/W^0 的元素 $\alpha+V^0$ 与 $\beta+W^0$ 定义

$$\overline{f}(\alpha+V^0,\beta+W^0)=f(\alpha,\beta),$$

证明这个定义是合理的，且 $\overline{f}\in P(V/V^0,W/W^0)$.

(iv) 证明 $\mathrm{d}(V/V^0)=\mathrm{d}(W/W^0)$.

11. (定理 7 的后一半) 设 V 与 W 是域 F 上线性空间. 证明存在一同构映射 φ : $V\otimes W\to W\otimes V$ 使

$$\varphi(\alpha\otimes\beta)=\beta\otimes\alpha,\quad \alpha\in V,\beta\in W.$$

12. 设域 F 上线性空间 V 有直和分解

$$V=V_1+V_2.$$

令

$$\widetilde{V}_1=\{f\in V^*\mid f(V_2)=0\},$$
$$\widetilde{V}_2=\{f\in V^*\mid f(V_1)=0\}.$$

证明 $V^*=\widetilde{V}_1+\widetilde{V}_2$ 且 $\widetilde{V}_1\cong V_1^*,\widetilde{V}_2\cong V_2^*$.

13. 设 A 为域 F 上 $n\times n$ 矩阵， B 为 $m\times m$ 矩阵. 证明：

(i) $A\otimes B$ 与 $B\otimes A$ 相似;

(ii) $|A\otimes B|=|A|^m|B|^n$.

14. 设 V 是域 F 上一 n 维线性空间. 定义映射

$$\varphi : V^* \otimes V \to \mathrm{Hom}(V, V)$$

为

$$\left(\varphi\left(\sum_{i=1}^{r} f_i \otimes \alpha_i\right)\right)(\beta) = \sum_{i=1}^{r} f_i(\beta)\alpha_i.$$

证明: φ 为一同构映射, 且

$$\mathrm{tr}(\varphi(f \otimes \alpha)) = f(\alpha),$$

其中 tr 表示线性变换的迹.

15. 设 V_1, V_2, W_1, W_2 是域 F 上的有限维线性空间. 定义双线性映射 $\varphi : P(V_1, V_2) \times P(W_1, W_2) \to P(V_1, V_2, W_1, W_2)$ 为

$$\varphi(f, g)(\alpha_1, \alpha_2, \beta_1, \beta_2) = f(\alpha_1, \alpha_2)g(\beta_1, \beta_2).$$

证明

$$P(V_1, V_2) \otimes P(W_1, W_2) \cong P(V_1, V_2, W_1, W_2),$$

其中 $\alpha_i \in V_i, \beta_i \in W_i, i = 1, 2$.

16. 设 V 是域 F 上任一线性空间, S 为 V 的一个子集合. S 称为 V 的一组基, 如果

(i) S 的任意一个有限子集合都线性无关;

(ii) V 中每一个向量都可以表成 S 中有限多个向量的线性组合.

设 V_r 是 n_r 维线性空间, 而 $\varepsilon_{r_1}, \cdots, \varepsilon_{r_{n_r}}$ 是 V_r 的基, $r = 1, 2, \cdots$. 作直和 $V = \sum_{r=0}^{\infty} V_r$. 证明集合

$$S = \{\varepsilon_{r_1}, \cdots, \varepsilon_{r_{n_r}}, r = 1, 2, \cdots\}$$

是 V 的一组基.

17. 设 V 是域 F 上一有限维线性空间. 证明 V 的张量代数 $T(V)$ 无零因子.

18. 设域 F 的特征为 0, V 是域 F 上一有限维线性空间. 对于 $x \in T_r(V)$, 定义

$$\mathrm{sym}(x) = \frac{1}{r!} \sum_{\sigma \in S_r} \sigma(x).$$

证明:

(i) $\mathrm{sym}\sigma = \sigma\mathrm{sym} = \mathrm{sym}$;

(ii) $\mathrm{sym}^2 = \mathrm{sym}$;

(iii) $\mathrm{sym}x = x$ 当且仅当 $\sigma(x) = x$, 对所有的 $\sigma \in S_r$.

19. 设域 F 的特征为 0, V 是域 F 上一有限维线性空间. 对于 $x \in T_r(V), y \in T_s(V)$, 证明:

$$\mathrm{Alt}_{r+s}(\mathrm{Alt}_r(x) \otimes y) = \mathrm{Alt}_{r+s}(x \otimes \mathrm{Alt}_s(y)) = \mathrm{Alt}_{r+s}(x \otimes y).$$

20. 符号同上. 在 $T(V)$ 中用 I 代表线性变换 Alt 的核, 即

$$I = \{x \in T(V) \mid \text{Alt}(x) = 0\}.$$

证明:

(i) I 是 $T(V)$ 的一个双边理想;

(ii) $I \cap E(V) = \{0\}$;

(iii) $T(V) = I \oplus E(V)$;

(iv) $E(V) \cong T(V)/I$.

21. 设域 F 的特征为 0, V 是域 F 上一 n 维线性空间, $\varepsilon_1, \cdots, \varepsilon_n$ 是 V 的一组基. 对于任意取定的 $x \in E_{n-r}(V)$, 对于任意的 $y \in E_r$, 其中 $0 < r < n$, 我们有

$$x \wedge y = f_x(y)\varepsilon_1 \wedge \cdots \wedge \varepsilon_n,$$

证明:

(i) f_x 是 $E_r(V)$ 的一个线性函数;

(ii) 映射 $x \mapsto f_x$ 是 $E_{n-r}(V)$ 到 $E_r(V^*)$ 的一个同构映射.

参考文献

[1] 范德瓦尔登 B L. 代数学 (I). 丁石孙, 曾肯成, 郝钢新译. 北京: 科学出版社, 1963

[2] 范德瓦尔登 B L. 代数学 (II). 曹锡华, 曾肯成, 郝钢新译. 北京: 科学出版社, 1976

[3] 贾柯伯逊 N. 抽象代数学 (I-III). 黄缘芳译. 北京: 科学出版社, 1960

[4] Jacobson N. 基础代数 (I). 上海师范大学数学系代数教研室译. 北京: 高等教育出版社, 1989

[5] Jacobson N. Basic algebra(II). W. H. Freeman and Company, 1980

[6] 莫宗坚, 蓝以中, 赵春来. 代数学. 北京: 北京大学出版社, 1986.

[7] 刘绍学. 近世代数基础. 北京: 高等教育出版社, 1999

[8] 柯斯特利金 A И. 代数学引论 (上、下). 张顺燕, 蓝以中, 丘维声译. 北京: 高等教育出版社, 1988

[9] 徐明曜, 黄建华, 李慧陵等. 有限群导引 (上、下). 北京: 科学出版社, 1999

[10] 阿丁 E. 伽罗华理论. 李英译. 上海: 上海科技出版社, 1958.

[11] 马力茨夫 A И. 线性代数基础. 柯召译. 北京: 高等教育出版社, 1957

[12] HALMOS P R. Finite dimensional vector spaces. Springer-verlag, 1953

索 引

一 画

二 画

三 画

四 画

五　画

六 画

七 画

十　画

十 一 画

十 二 画

十 三 画

十 四 画

十 六 画